Authentication and supervision: A survey of user attitudes

S.M. Furnell, P.S. Dowland, H.M. Illingworth and P.L. Reynolds

Abstract

User authentication is a vital element in ensuring the secure operation of IT systems. In the vast majority of cases, this role is fulfilled by the password, but evidence suggests that this approach is easily compromised. Whilst many alternatives exist, particularly in the form of biometric methods, questions remain over the likely user acceptance. This paper presents the results of a survey that examines user attitudes towards a range of authentication and supervision techniques. It is concluded that whilst there is still an element of reluctance amongst users to depart from the familiar password based mechanisms, many are convinced of the need for improved authentication controls. The acceptability to users of various new techniques is variable, but many seem willing to consider a range of alternative methods.

Keywords

Authentication, Biometrics, User supervision, Survey.

Introduction

User authentication is widely accepted to represent an essential first line of defence in the security of Information Technology (IT) systems. All but the most trivial systems, therefore, require some form of authentication in order to verify that a claimed user identity is indeed correct. There are three main approaches to user authentication: something the user knows (e.g. password or PIN), something the user has (e.g. a card or other token) and something the user is (e.g. a biometric characteristic) [1]. By far the most commonly used means of authentication in IT systems is the password. Passwords are conceptually simple for both system designers and end users, and can provide effective protection if they are used correctly. However, the protection provided is often compromised by users themselves. Typical problems include forgetting passwords, writing them down, sharing them with other people and selecting easily guessed words.

If the password approach is to be replaced or supplemented, then alternative means of authentication are clearly required. However, when considering such alternatives, a number of factors can be cited that may complicate their adoption:

- effectiveness (i.e. the ability to detect impostors, whilst allowing legitimate access);
- cost (i.e. financial overheads of deployment);
- user acceptance (i.e. the friendliness and transparency of the measure).

Of these, the issue of user acceptance is possibly the most difficult to assess, as it represents a highly subjective measure. This paper presents the results from a survey that set out to assess public attitudes to various forms of user authentication and, thereby, determine whether acceptable alternatives to the password could be identified. The discussion begins by summarising the potential problems with existing password approaches and then proceeds to consider the alternatives that are offered by various classes of biometric method. Details of the survey itself are then presented, leading into an analysis of the results obtained.

The problems with passwords

The password approach has a number of shortcomings, which can undermine the effectiveness of the approach [2]. Indeed, passwords can often be considered a mere hindrance to a determined hacker and can easily be bypassed by relatively inexperienced individuals using tools freely available on the Internet.

Several studies have been carried out over the last 20 years looking at the ease with which passwords can be determined. In 1979, 86% of the 3829 passwords gathered, could be guessed by a PC in less than one week [3]. This was later repeated by Klein in 1990 [4] and Spafford in 1992 [5]. Whilst the results from these subsequent experiments showed that password selection had improved (only 21% could be guessed in a week), so have the tools that can be used to *guess* them. In 1998, L0pht Heavy Industries released L0phtCrack [6], a utility which allows Windows NT Server Message Block (SMB) password packets to be captured during network authentication sessions. This utility not only allows the encrypted passwords to be captured directly off the network, it can also perform a dictionary and brute force attack against the encrypted passwords. Similar utilities are also available for other operating systems - most notably CRACK which runs under a number of flavours of UNIX [7].

There are a number of measures that can be taken to improve password security. For example:

- *Non-Dictionary words*. Forcing users to select non-dictionary passwords prevents the use of dictionary based attacks. Such attacks can identify a password in less than 20 minutes even on dictionaries with up to one million words. The only way to identify non-dictionary passwords is using a brute-force approach (testing every combination of characters for every length of password).
- *Passwords with mixed case/symbols*. Including both upper/lower case and symbols (!£$% etc.) in passwords requires any attack to use a brute force method and increases the number of character permutations that must be tried.
- *Password ageing*. Should an intruder obtain a valid username/password combination, most systems will allow them to continue to access the system until the intrusion is noticed. If a password ageing policy is in place users can be forced to change their passwords regularly, thus forcing the intruder to identify the new password.

Although these sugestions will help to make a password-based system more resiliant to an intruder they are by no means secure. A determined intruder can utilise password cracking utilities to determine even the most random password in a matter of weeks. With the advent of more powerful processors, intruders can crack passwords in a more realistic time – a matter of days for some PCs. In addition, it can be argued that restrictions such as those above may compromise the simplicity (and, hence, user friendliness) of the password method – one of the previously cited advantages. To counter these problems with password based systems, it is necessary to consider alternative approaches to user authentication.

An overview of biometric authentication approaches

Whereas the password approach relies upon something the user *knows*, biometric authentication is based upon something the user *is*. This has the advantage that it is less straightforward for the user to be impersonated or to compromise protection themselves (e.g. they cannot share, write down or forget a biometric characteristic).

Methods of biometric authentication fall into two distinct categories, namely physiological and behavioural characteristics [8].

- Physiological biometrics represent those traits that describe who we are based on physical attributes, for example fingerprints, hand geometry, retinal and iris scanning. These characteristics usually require additional equipment to be connected externally to the computer to provide the necessary data capture.

- Behavioural biometrics encompass attributes such as typing style, voice pattern and signature recognition. Most behavioural characteristics can be acquired without the need for external equipment (e.g. keyboard & mouse), although some do require specialised hardware solutions (e.g. signature recognition).

Most biometric devices offer a compromise between high security/low user acceptance and low security/high user acceptance. This trade-off can be measured as the False Acceptance Rate (FAR) and False Rejection Rate (FRR) of the devices. It has so far proved impossible to achieve a system where the FAR and FRR are simultaneously reduced to zero, as they share a mutually exclusive relationship [9]. Most systems select an appropriate level at which inconvenience to the user, through denial of access (false rejections), is acceptable, without allowing too many intruders unauthorised access (false acceptances). All systems have an Equal Error Rate, the point at which the FAR and FRR rates are equal. Whilst this rate represents the theoretical "best-fit" for security measures, it is rarely ideal in a secure environment where a preference for either high FAR or FRR exists.

In recent years, biometric techniques have progressed from the research environment to consumer products. Indeed, Microsoft Windows now incorporates a biometric application programming interface to enable easy integration and utilisation of such approaches within the operating system [10]. Some biometrics are, however, more mature and well-known than others. The table below presents a list of biometric

techniques and accompanying descriptions (these descriptions are worded as presented to the respondents in the survey that is described in the next section).

Method	Description
Keystroke analysis	Research has shown that users have different typing styles and that they can be identified by measuring the times between keystrokes [11].
Face recognition	A snapshot of the user, taken by a camera positioned on the monitor, is compared with a previously stored 'faceprint'.
Mouse dynamics	Similar to keystroke analysis, users can be identified by the way in which they use the mouse.
Voice verification	A user's voice, when speaking a word or phrase into the computer's microphone, is compared with a previously stored 'voiceprint'.
Signature analysis	A user signs their name using a special pen and pad, the signature is digitised and compared with a previously stored version.
Iris scanning	A snapshot of the user's iris, taken by a camera, is compared with a previously stored image.
Hand geometry	This technique measures the physical dimensions of the hand using a small camera and compares these with previously stored values.
Fingerprint analysis	An automated version of the fingerprint identification system similar to that traditionally used in criminology.

Table 1 : Biometric methods, as presented to survey respondents

Many organisations are already testing such alternative forms of user authentication. For example, trials of iris recognition systems have been conducted in the banking sector for use in automated teller machines [12].

A subset of the above biometrics (e.g. keystroke analysis, mouse dynamics) can be considered to represent aspects of the wider issue of behaviour monitoring. This recognises that everyone has characteristic ways of doing things and that, over time, it may be possible to establish individual profiles of behaviour. IT systems offer a number of factors that may be monitored in order to establish such a profile. Examples include:

- typical access time and location;
- operating system command usage;
- typical application and resource utilisation;
- methods of user interaction.

Techniques such as these have been incorporated into a variety of intrusion detection and monitoring systems, which can provide real-time supervision of user activity in order to detect potential impostor activity and other forms of misuse [13]. Although such an approach represents an increase in the level of security, there is also the potential to alienate legitimate users, who may be concerned about their activities being monitored to this level.

A significant body of work exists in relation to biometrics and behavioural monitoring systems and, as previously mentioned, many commercial products are now available as alternatives to simple passwords. It is, therefore, relevant to consider what the views of the potential users themselves are towards the technologies. This issue is explored in the sections that follow.

A Survey of attitudes towards authentication technologies

In order to determine the acceptability of user authentication and supervision techniques, a survey was conducted to assess the attitudes and awareness of the general public. The survey aimed to assess the following issues:

- public attitudes towards different forms of user authentication;
- the attitudes towards the concept of continuous monitoring.

The survey questionnaire consisted of 53 main questions, the majority of which were multiple choice, with the remainder requiring short written responses. Many of the questions contained multiple sections, resulting in a maximum of 130 possible answers per respondent. The survey was split into a number of categories, each focussing on a specific area of interest to the authors. Questions 1-7 gathered general details, to determine the gender, age, education, and level of computer use; these provided demographic information on the survey response base. Questions 8-14 considered the use of computers within the respondent's work environment, whilst questions 15-19 considered the use of computers at home. These helped to provide information on the spread of IT into the home and work contexts, as well as the likely IT awareness of the respondents. Questions 20-34 were intended to determine individual opinions and knowledge in the area of computer crime and abuse. The final section (encompassing questions 35-53) looked at the respondent's views on user authentication and supervision. This paper targets the issues of user authentication and supervision, whilst the findings relating to computer crime have been documented in a previous publication [14].

The survey was distributed to a wide range of individuals and organisations with the intention of gaining a diverse variety of opinions. The questionnaire was made available in two forms, a printed copy and an online version published on the authors' WWW site. Approximately 300 printed surveys were distributed with 148 completed responses being received, representing a response rate of 49%. A further 27 surveys were submitted via the web site resulting in a total of 175 responses. It should be noted that, whilst questionnaires were sent to companies, the focus required respondents to reply from an individual rather than organisational perspective. As

such, these responses were still representative of a public rather than business viewpoint on the issues.

Analysis of results

General

The vast majority (80%) of the survey respondents were male. In terms of age, 74% of the respondents were below 35, indicating that the vast majority of the responses were likely to be from people who had 'grown up' with IT to some extent. The overall breakdown of respondents by age group is given in table 2.

Age range	Respondents
16 to 24	42%
25 to 34	32%
35 to 49	18%
50 to 64	7%
65 and over	0%

Table 2 : Survey respondents by age

In terms of employment background, a high number of responses were received from the technology fields (with 103 out of the 175 responses claiming to be from the computing, communications or engineering domains). Academically over 70% of the respondents claimed to hold post-16 qualifications, with 44% having a degree level education. This represents a high level of academic achievement among the respondents and reflects the fact that the distribution of a large proportion of surveys occurred via academic channels.

The respondents had considerable familiarity with IT, with over 98% having used a computer for over one year, 88% using a computer at work and 84% using one at home. The respondents were also asked about the availability of Internet access. 129 respondents (88%) claimed to have access at work, while 69 respondents (48%) claimed to have access at home.

The information above indicates that the respondents were generally IT literate and had considerable experience using computers in both home and work environments. As later sections of the survey looked at views on user authentication and supervision in relation to such systems, it was felt that the respondents were suitably qualified to comment on these issues.

Password based authentication

Given that they represent the most common (and, hence, familiar) form of authentication, the survey began by assessing respondent attitudes towards passwords. The results indicated that over 91% of respondents relied on passwords for access

control to their computers, a figure that is generally compatible with the 1998 KPMG security survey, which showed 97% of organisations using them [15].

Due to the dominance of passwords, most users have multiple passwords for different systems and applications. When asked how many different systems or applications they use which require passwords, 26% of respondents claimed to have five or more, with 18 people claiming in excess of ten (see figure 1).

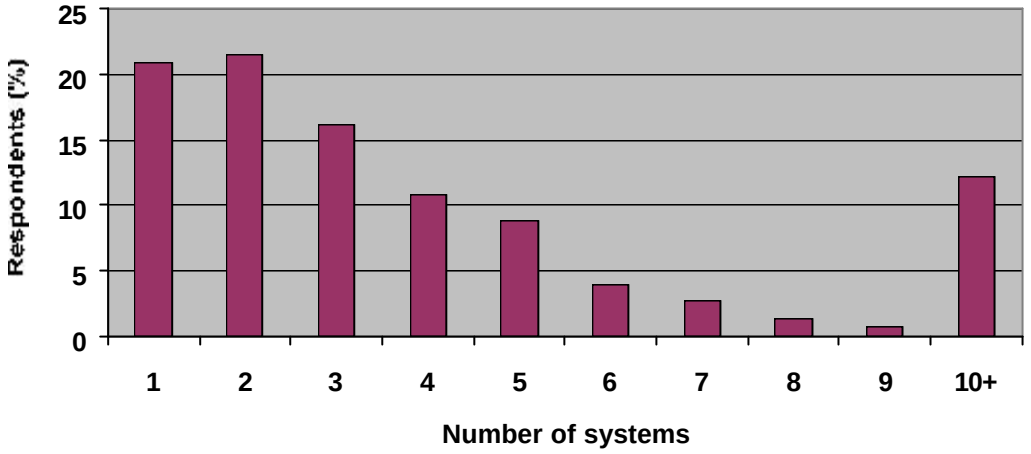

Figure 1 : Number of different systems/applications used requiring passwords

The requirement to remember such a large number of passwords can cause a major problem for users. It is, therefore, no surprise that users often select dictionary words or personal names as the basis for their passwords, as these are easier to remember. Having said this, only 15% of respondents felt that their passwords could be easily guessed. The phrasing of the question in this case gave examples of information that, if used as a basis for selection, could render the password more easily guessed (i.e. "is it part of your address, name, partner's name?"). Although the majority of users considered themselves to be safe on this basis, the question did not provide an exhaustive list of what might constitute obvious choices. As such, many respondents may still have been using insecure passwords, such as dictionary words (which the aforementioned L0phtCrack tool can determine in less than a minute).

Not only do users often choose insecure passwords, they also frequently select the same password for multiple accounts, with 40% of respondents re-using the same password. As such, should an intruder gain access to one protected account, it is quite likely that he/she will be able to reuse that same password for other machines and applications. A further issue is that of the password's lifetime. Once a password is illegitimately acquired then, without time limits, restricted logins or account monitoring, it is possible that the intruder would remain unnoticed until he/she committed an act that caused some form of disruption. The respondents were asked how frequently they changed their passwords and if they were forced to change their passwords by the system or the system administrators. As indicated in table 3, an alarming 34% of respondents claimed to never change their passwords. Furthermore, the responses to the subsequent question revealed that 51% were not forced to change their password by the system. The former represents bad practice on the part of the users, whereas the latter reflects poor system administration. From an administration

point of view, it is more encouraging to observe that 70% of users claimed to use systems in which a minimum password length is enforced. Having a minimum length of seven or more characters helps to ensure that passwords are more resilient to brute force attacks.

Frequency of password change	Respondents
Weekly	2%
Fortnightly	1%
Monthly	25%
Six-monthly	18%
Less frequently	20%
Never	34%

Table 3 : Frequency of password changes

Responses to subsequent questions revealed that, in many cases, the respondents themselves were compromising password protection, with 15% admitting to writing them down and 29% willingly sharing them with colleagues. In addition to this, 31 (21%) of the 151 respondents who used computers at work claimed to have used another person's password without their consent or knowledge.

These results serve to underline some of the known problems with passwords and provide the justification for the subsequent questions, which asked users about other forms of authentication.

Alternative authentication and supervision methods

One of the main objectives of the survey was to evaluate user's opinions regarding different authentication methods. In order to achieve this, the respondents were asked to rate the acceptability of a variety of initial login and continuous supervision techniques on a 5-point sliding scale from 'totally acceptable' to 'totally unacceptable'. A total of nine methods were cited, ranging from passwords to a variety of physiological and behavioural biometric methods. Each of the methods was briefly described on the questionnaire sheet to ensure that the respondents understood the context (using the text previously shown in table 1). Table 4 summarises the ranked results, which are also illustrated graphically in figure 2. The responses have been normalised to reflect the variable response rate to each question, as there was a higher response rate to questions on initial login authentication (probably reflecting a lack of understanding of the concept of continuous supervision amongst some respondents). The positive responses ('totally acceptable' and 'acceptable') were summed and then the total number of negative responses ('unacceptable' and 'totally unacceptable') were subtracted, thus producing a rank of user preference.

Method	Initial login authentication	Continuous supervision
Password	95.7%	-10.2%
Keystroke analysis	29.8%	25.5%
Face recognition	49.1%	3.2%
Mouse dynamics	21.3%	21.8%
Voice verification	53.4%	-0.6%
Signature analysis	40.1%	-35.9%
Iris scanning	47.2%	-16.8%
Hand geometry	44.4%	-19.9%
Fingerprint analysis	48.8%	-16.0%

Table 4 : Ranked user preference of security methods

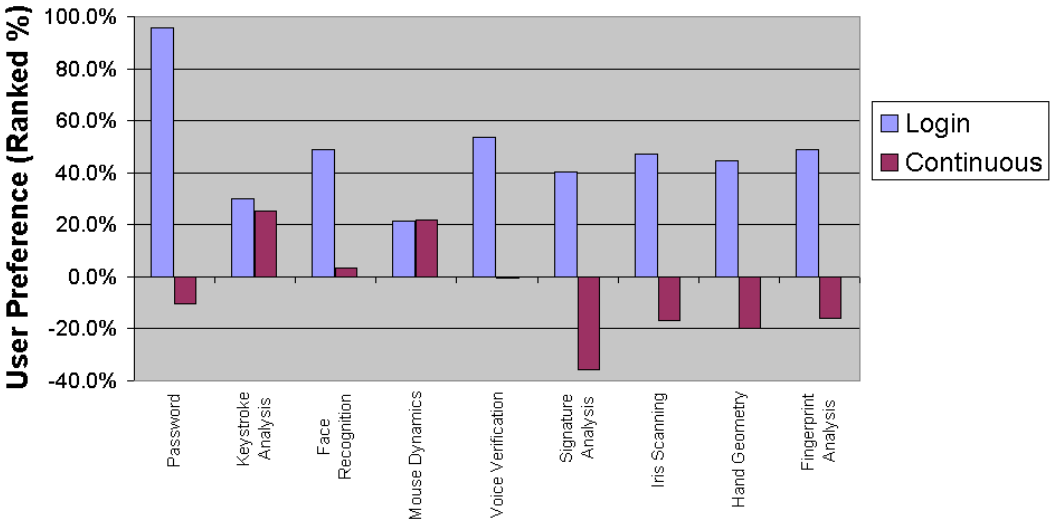

Figure 2 : User preference of authentication methods

As expected, the most popular form of initial login authentication was the password, with 90% of respondents rating it as 'totally acceptable' (scoring more than twice as many votes in this category than most other methods). However, this did not mean the outright rejection of alternative methods and many also achieved respectable scores. The authors were, however, surprised to see a general acceptance of mouse dynamics for initial login authentication. This was felt to be somewhat erroneous, as it is unlikely that moving the mouse for logging-on would provide sufficient data for a unique identification. It is expected that using a combination of methods, such as password and keystroke analysis, would provide a much more reliable method of initial login authentication.

It is clear that there is a high level of user acceptance for all the initial login authentication techniques suggested. Methods such as face recognition, voice verification, signature analysis, iris scanning, hand geometry and fingerprint analysis were all considered favourably. It is interesting to note that all of these techniques (with the exception of signature analysis) have had significant media coverage,

especially through film and television. It is possible that familiarity with these techniques influenced the respondents' choices. The acceptance of signature analysis cannot be readily explained by the familiarity with the technology through the media, however the concept of a signature as a means of identity verification is well established in our society.

After passwords, the most acceptable forms of login authentication were considered to be voice verification and fingerprint recognition, scoring raw overall acceptability ratings of 68% and 67% respectively. The latter result is somewhat surprising, in that conventional wisdom suggests that the association of fingerprints with criminal identification may represent a potential barrier to user acceptance. However, it is clear from these results that the majority of respondents are comfortable with the concept. It can, however, be noted that, in the normalised results (as presented in table 2), face recognition scored higher than fingerprints once negative responses had been taken into account

One of the significant questions posed in the survey was whether respondents would be comfortable with the concept of continuous supervision. This would provide a means for authentication to become an ongoing process within a logged in session, rather than being merely a one-time judgement at the beginning. This, in turn, would guard against situations such as an impostor replacing a legitimate user at the terminal or an impostor who may have been able to fool the initial login authentication system. In general, the respondents were positive towards the idea of monitoring, with 43% considering it acceptable, though 29% were unsure. However, the respondents considered only three techniques acceptable; namely keystroke analysis, mouse dynamics and face recognition (the latter being with a very low preference). Whilst the overall ranked results reflected sensible views, some of the individual responses in the underlying data did provide a few surprises. In particular, 34 respondents rated the use of signature analysis for continuous monitoring to be 'acceptable'. This is most likely to be a misunderstanding, as few computer users would be prepared to stop work and sign their name intermittently (a view borne out by the fact that 90 rated this as 'unacceptable').

Respondents were also asked to consider how long they would be prepared to spend creating a behaviour profile that the monitoring system would use to authenticate them. The responses are shown in table 5. It is clear that the majority of users would not be tolerant of explicit profiling activity for any long periods. Equally, the time that most of them would consider acceptable is 15 minutes or less – which would be unlikely to be adequate for some measures (e.g. whilst face and fingerprint recognition systems would allow adequate registration within this time, accurate measures relating to typing and more general system usage would require longer periods). As such, elements of profiling would need to occur as a transparent background task in order to ensure user acceptance.

User-profile set-up time	Respondents
No time	11%
Up to 5 mins	36%
Up to 15 mins	24%
Up to 30 mins	13%
Up to 1hr	12%
> 1hr	5%

Table 5 : Acceptable duration of profiling activity

Once a profile has been created, there is still the possibility that a monitoring system may falsely reject a legitimate user, believing them to be an impostor. The questionnaire made the respondents aware of this and asked them how frequently they would be willing to tolerate such errors. The results are presented in table 6 and clearly illustrate that any deployed system would need to have a very low error rate in order to avoid alienating the user population.

Frequency of false rejection	Respondents
Hourly	7%
Daily	27%
Weekly	36%
Never	29%

Table 6 : Perceived tolerable frequency of false rejection by monitoring system

It is recognised that the concept of continuous supervision also introduces ethical considerations. Indeed, 40% stated that they would consider monitoring as an invasion of their privacy, with a further 18% being unsure. It is clear that if continuous supervision of users is to be implemented, then certain safeguards should be considered. In particular, users should be aware of the intended uses of the information collected. 45% of respondents felt that they could not trust their organisation to use the supervision data for security-related purposes only and were concerned that it could be utilised for an ulterior motive, such as monitoring work productivity. 85% stated that users should be aware of any monitoring being used. The simplest way to ensure these requirements are met is to involve the users in the planning and implementation of these systems and provide clear policies on the uses for the gathered information.

Finally, the respondents were asked to indicate which fields/sectors would benefit most from supervision of users by computer, rating the benefit from ‘great benefit’ to ‘no benefit at all’. These results were collated and ranked and are shown in figure 3.

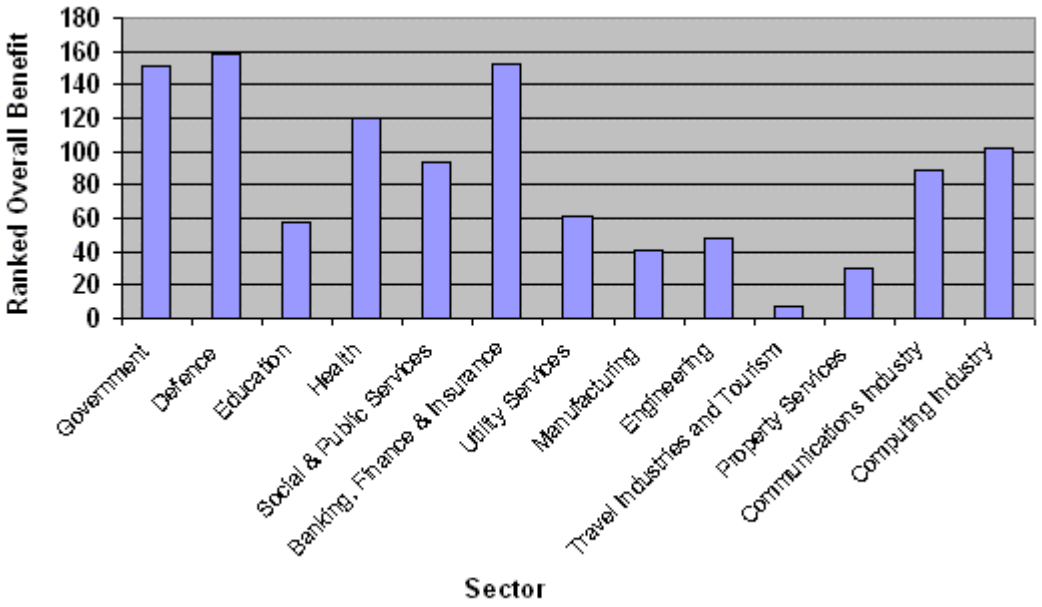

Figure 3 : Benefit from monitoring by sector

As expected, the majority of respondents considered the areas of government, defence, health and banking to benefit most from user supervision (these being the areas with the most obviously sensitive systems and data to protect). However, the respondents felt that all areas could benefit from improved supervision, showing that there is still considerable concern over the perceived computer security across all sectors.

Discussion

The results clearly demonstrate the shortcomings of password-based authentication, as well as the fact that, in spite of these, it remains the dominant form of user authentication. However, the fact that the respondents have shown a willingness to use alternative authentication techniques can be considered to be encouraging. It should be noted, however, that in the majority of cases, it is unlikely that the respondents had actually used the techniques that they were being asked to comment upon. As such, it is possible that their views may change if presented with the practical experience.

Given that a strong preference was expressed for passwords, consideration should be given to retaining them as the means of login authentication, whilst identifying means to compensate for their weaknesses. Suitable strategies in this respect could include:

- Utilising password login in conjunction with transparent keystroke analysis of the information entered. In this way, the user would be authenticated not only by *what* they type, but also *how* they type it. This should not have any significant influence on user acceptance, as the primary authentication mechanism will still appear to be the password.

- Retaining password-only authentication at login, but supplementing it with continuous supervision during the user session. The survey results suggest that techniques such as keystroke analysis and mouse dynamics would be acceptable to users in this regard.

The respondents preference for passwords is in agreement with the previously published results from the Australian TRUST project, which (from a survey of 76 participants) found users' principal preference to be for passwords, followed by physiological biometrics and, finally, behavioural measures [16]. The latter finding is, however, in contrast to the results from this study in that (for continuous monitoring) the behavioural techniques of keystroke and mouse dynamics were chosen in preference to the physiological technique of face recognition. Indeed, in the TRUST study, keystroke analysis and pointing device based verification scored the lowest of the seven biometrics assessed.

Although many considered the concept of continuous supervision to be acceptable for security purposes, the respondents showed concern over the potential wider use of such data. As such, it is important for organisations to establish agreed working practices to employees before proceeding with such methods (this may assist in reassuring those such as the 29% of respondents who were undecided over the acceptability of the monitoring concept). If such practices are not naturally adopted by organisations, it is possible (maybe even preferable in some cases) to legislate on acceptable supervision practices. This could be implemented in a similar way to that which restricts the rights of an employer to intercept and/or read an employee's email correspondence.

Overall, a significant factor in the acceptance of alternatives to the password will be that of education. If people can be shown that newer authentication techniques are safe, reliable and secure, then their acceptance is likely to be improved.

Conclusions

The survey has shown that, although demonstrably weak, the password remains the most popular form of authentication in the minds of users. However, a number of other methods emerged as possible contenders and it is possible that practical experience of using them, combined with improved awareness of the vulnerabilities of passwords, would increase their perceived acceptability as alternatives.

Another conclusion that can be drawn from the survey results is that the use of continuous supervision is, in general, acceptable. However the viability of such a scheme would be dictated by the methods chosen and subject to suitable assurances being given to the monitored population regarding the planned uses of the collected data.

The findings from the survey will be used to inform on-going work in relation to an architecture for real-time user supervision and monitoring [17]. This system will be based upon composite authentication techniques, rather than attempting to apply particular techniques in isolation.

References

[1] Wood, H.M. 1977. “The use of passwords for controlled access to computer resources”, NBS Special Publications, U.S. Dept. of Commerce/NBS: 500-509.

[2] Jobusch, D.L. and Oldehoeft, A.E. 1989. "A Survey of Password Mechanisms : Part 1", Computers & Security, Vol. 8, No. 7: 587-604.

[3] Morris, R. and Thompson, K. 1979. “Password Security: A Case History”, Communications of the ACM, Vol. 22, No. 11: 594-577.

[4] Klein, D. 1990. “A survey of, and improvements to, password security”, Proceedings of the USENIX Second Security Workshop, Portland, Oregon, August 1990: 5-14.

[5] Spafford, E.H., 1992, “Opus: Preventing Weak Password Choices”, Computers and Security, Vol. 11, No. 3: 273-278.

[6] Heskett, B. 1998. “A new windows password cracker”, Cnet News.com, 13th February 1998, http://news.cnet.com/news/0-1003-200-326537.html

[7] Cherry, A., Henderson, M.W., Nickless, W.K., Olson, R. and Rackow, G. 1992. “Pass or Fail: A New Test for Password Legitimacy”, Mathematics and Computer Science Division, Argonne National Laboratory, MCS-P328-1092, September 25th 1992.

[8] Sherman, R. 1992. “Biometrics Futures”, Computers & Security, vol. 11, no. 2: 128-133.

[9] Cope, B.J.B. 1990. "Biometric Systems of Access Control", Electrotechnology, April/May: 71-74.

[10] Sapsford, J. 2000. “Biometrics to bolster Windows security”, ZDNet News, 2 May 2000.

[11] Furnell, S.M., Morrissey, J.P., Sanders, P.W., and Stockel, C.T. 1996. “Applications of keystroke analysis for improved login security and continuous user authentication”, Katsikas and Gritzalis (eds), Proceedings of 12th International Conference on Information Security (IFIP SEC ‘96): *283-294*.

[12] NCR. 1999. “NCR announces iris recognition trials with Nationwide Building Society”. http://www3.ncr.com/product/financial/press/sensnat.htm

[13] Mukherjee, B., Heberlein, L.T., Levitt, K.N. 1994. “Network Intrusion Detection”, IEEE Networks, Vol. 8, No. 3: 26-41.

[14] Dowland, P.S., Furnell, S.M., Illingworth, H.M., and Reynolds, P.L. 1999. “Computer Crime and Abuse: A Survey of Public Attitudes and Awareness", Computers & Security, vol. 18, no. 8: 715-726.

[15] KPMG. 1998. *Information Security Survey 1998*, KPMG Information Risk Management, UK, http://www.kpmg.co.uk.

[16] Deane, F., Barrelle, K., Henderson, R., and Mahar, D. 1995. “Perceived acceptability of biometric security systems”, Computers & Security, vol. 14, no. 3: 225-231.

[17] Furnell, S.M. and Dowland, P.S. 2000. "A conceptual architecture for real-time intrusion monitoring", Information Management & Computer Security, vol. 8, no. 2.