December 2005

An Empirical Study of User Practice in Password Security and Management

Kay Bryant
Griffith University

John Campbell
University of Canberra

An Empirical Study of User Practice in Password Security and Management

Kay Bryant
John Campbell
Griffith University
University of Canberra

Griffith Business School
Griffith University
Brisbane, Queensland
Email: k.bryant@griffith.edu.au

School of Information Sciences and Engineering
University of Canberra
Canberra, Australian Capital Territory
Email: john.campbell@canberra.edu.au

Abstract

Maintaining the security of information systems and associated data resources is vital if an organisation is to minimise losses. Access controls are the first line of defence in this process. The primary function of access controls is to restrict the use of information systems and resources to authorised users. Password-based systems remain the predominant method of user authentication despite the many sophisticated and viable security alternatives that have emerged from research and development. However, evidence suggests that passwords as a means of authentication is often compromised by poor security practices. This paper presents the results of a survey that examines user practice in creating and using password keys and reports the findings on user password composition and security practices for e-mail accounts. Despite a greater awareness of security issues, the results show that an improvement in user password management practice is required.

Keywords

User authentication, password composition, password management, password security, password reuse

INTRODUCTION

Organisations, governments and even individuals increasingly rely on information technology for day-to-day activities. However, this reliance comes at a cost especially if information assets are to be protected. Maintaining security over application systems and databases is essential if losses, intentional or otherwise, are to be eliminated or at the very least minimised. Establishing security on the boundary of a system is the first step in minimising losses. Boundary controls are typically implemented through system hardware and software (Weber, 1999). Access controls are the usual type of control implemented on the boundary of a system. The primary function of these controls is to restrict the use of systems and resources to authorised users. Access controls also limit the type of actions that a user can perform and ensure that users can only obtain access to authentic information systems and resources. Implementing access controls is a relatively straightforward process when there is only a single user. However, as organisations of today have multiple users as well as multiple applications the task of protecting resources is more expensive.

Access control mechanisms are typically part of the operating system. However, given the extent of the organisational networks and their connection to the Internet, specialised software such as firewalls are used to implement basic access control functions (Oppliger, 1997). Controlling access to system resources is usually a three-step process. Firstly, users identify themselves to the mechanism, then they must authenticate themselves and the mechanism authenticates itself. Lastly, users request information technology resources and the actions they will take and the mechanism will either permit or deny the request based on information held on file denoting the resources and actions a user is permitted to undertake. The means by which users make themselves known to the system is typically through a unique identifier such as a name or an account number. Once the access control mechanism establishes that it has a valid user, authentication of that user is undertaken. Password systems are the most commonly used means of authentication in computer-based systems. Unfortunately, users can compromise password security by forgetting passwords, writing them down, sharing them with other people and selecting easily guessed words.

This paper explores the means by which a system authenticates users as well as outlining problems associated with the most common approach that is, passwords. Lastly, the results of a study examining user practices in creating and maintaining passwords are provided.

APPROACHES TO AUTHENTIFICATION

There are three main approaches to user authentication: something the user remembers (password or PIN), something the user has (a smart card or other token) and some physical characteristic of the user (fingerprint, retinal image and so on) (Furnell et al., 2000). Each approach has intrinsic flaws and these will be discussed in turn.

Remembered information can simply be forgotten so users typically resort to using information that is easy to recall. One consequence of this is that while the information is easy to recall, it is also relatively easy to guess. Passwords that are more difficult to remember may be written down thereby compromising the password and system security. Further, due to the predominance of password authentication systems, many users are required to remember passwords for a range of different systems and applications. The requirement to remember such a large number of passwords can cause a major problem for users. It is, therefore, no surprise that users frequently select dictionary words or personal names as the basis for their passwords, as these are easier to remember. Not only can users choose insecure and easily guessed passwords, they may also select the same password for multiple accounts. As such, should an intruder gain access to one protected account, it is quite likely that he or she will be able to reuse that same password to gain access to other devices or applications. Once a password is compromised, an intruder may remain unnoticed for some time unless passwords are changed frequently.

Possessed objects include such items as smart cards, swipe cards, keys, tokens, badges and rings can be misplaced, lost or stolen. The protection of systems using this approach requires the user to notify the appropriate authorities if the item is lost. Failure to do this compromises security since the system is unable to determine if the possessor is a valid user or not. Once notified of a lost or stolen object, the control mechanism denies all requests made using that object. Other steps may also be undertaken. The system should log details of the request, retain the object and it may even sound an alarm. Personal characteristics such as fingerprints, voiceprints, retinal or iris images and hand size, are difficult to replicate and thus are an effective means of authenticating users. However, the devices needed to capture the data and subsequently identify users are expensive to implement. Regardless of the approach to user authentication selected, organisations trade-off the value of the resources being protected and the effectiveness and cost of implementing and maintaining it. Passwords are the most common means of authenticating a user as they are conceptually simple for both system designers and end users, and can provide effective protection if they are used correctly. Issues associated with passwords are discussed in the following section.

PASSWORD SECURITY ISSUES

The password approach has a number of shortcomings, which can undermine the effectiveness of the approach (see for example Jobusch and Oldehoeft 1989, Furnell et al. 1999, Conklin et al. 2004, Carstens 2004, Ives et al. 2004). Several studies have examined the ease with which passwords can be determined. In one of the earliest empirical studies, Morris and Thompson (1979) found that a personal computer could guess 86 percent of passwords in less than one week. Subsequent replications of this study by Klein (1990) and Spafford (1992) found that password selection had improved over time with only 21 percent being able to be guessed in a week. Unfortunately, the software tools that can be used to deduce passwords have become even more powerful and seditious in recent years. The major strategies for overcoming the inherent weaknesses in password usage include the following:

- Non-Dictionary words: selecting 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 password, most systems will allow them to continue to access the system until the intrusion is noticed. Users need to change their passwords regularly, thus forcing the intruder to identify the new password.

While these strategies may help improve password security, these restrictions make the composition and memorising of passwords a complex and unintuitive exercise.

A SURVEY OF EMAIL PASSWORD SECURITY

E-mail research is part of the wider research field of computer-mediated communication (CMC) and is one of the most widespread CMC applications so far and affects the daily life of almost every working person in the industrialised world (Rudy 1996, Bälter 2000). While most research on e-mail usage has focused on issues of media choice and media effects (see Lee 1994, Markus 1994), it was concluded that e-mail systems would prove a useful survey context because of its importance and widespread social and organisational impact. Initially, a pilot study was undertaken to gain insight into password behaviours and to test the survey instrument (Authors, 2004). Once changes were made to the survey instrument based on the outcome of the pilot study, a more extensive study was conducted. The study was designed to assess the attitudes and awareness of the public and to gain insight into password composition and management practice. The study focused on the following issues:

- Profiling E-mail account usage (purpose, number of accounts, frequency of access)
- Password practice (reuse, composition, disclosure)

Consequently, a questionnaire was designed to elicit responses about student use and management of e-mail passwords. The first section of the questionnaire collected demographic data and information as to their computer and email usage. It also ascertained the extent to which they shared passwords across applications and their awareness of password cracking techniques. The second section focused specifically on password composition and management practices.

Undergraduate level students from an Australian university business faculty were chosen to be the research participants as the beliefs and practices of these business students may be echoed in their behaviour both as individual citizens and in their various positions in organisations. The survey was administered to the students in the first week of semester 1, 2005. All students were within the Business School and in their first year of study. In order to gain as many participants as possible, students from three different university campuses were asked to participant in the study. However, participation in the survey was entirely voluntary. In all, 884 students volunteered to participate in this study; 464 from the southern campus, 178 from the central campus and 242 from the northern campus. Table 1 shows the relevant demographic details for the participants, by campus and in total.

Table 1: Demographic Details of Participants

Variable	Category	Southern		Central		Northern		Total	
Age	< 18 years	120	25.9%	46	25.8%	47	19.4%	213	24.1%
	18 – 25 years	307	66.2%	113	63.5%	164	67.8%	584	66.1%
	26 – 35 years	22	4.7%	10	5.6%	23	9.5%	55	6.2%
	36 – 45 years	12	2.6%	6	3.4%	5	2.1%	23	2.6%
	46 – 55 years	2	0.4%	2	1.1%	2	0.8%	6	0.7%
	> 56 years +	1	0.2%	1	0.6%	1	0.4%	3	0.3%
Gender	Male	158	34.1%	96	53.9%	124	51.2%	378	42.8%
	Female	306	65.9%	81	45.5%	118	48.8%	505	57.1%
	No response	0	0.0%	1	0.6%	0	0.0%	1	0.1%
Enrolment Status	Full-time	429	92.5%	159	89.3%	223	92.1%	811	91.7%
	Part-time	28	6.0%	16	9.0%	15	6.4%	59	6.7%
	Not enrolled	1	0.2%	0	0.0%	0	0.0%	1	0.1%
	No response	6	1.3%	3	1.7%	4	1.7%	13	1.5%
Employment Status	Full-time	36	7.8%	15	8.4%	14	5.8%	65	7.4%
	Part-time	286	61.6%	110	61.8%	137	56.6%	533	60.3%
	Not employed	130	28.0%	47	26.4%	80	33.1%	257	29.1%
	No response	12	2.6%	6	3.4%	11	4.5%	29	3.3%
Computing Experience	0 – 2 years	11	2.4%	6	3.4%	8	3.3%	25	2.8%
	3 – 5 years	63	13.6%	21	11.8%	42	17.4%	126	14.3%
	6 – 10 years	257	55.4%	93	52.2%	130	53.7%	480	54.3%
	> 10 years	132	28.4%	58	32.6%	62	25.6%	252	28.5%
	No response	1	0.2%	0	0.0%	0	0.0%	1	0.1%
Participant	Totals:	464	52.5%	178	20.1%	242	27.4%	844	100.0%

Percentage totals may exceed 100% due to rounding.

Overall, the gender breakdown was 378 males and 505 females; one student did not respond to this question. There were marginally more males than females except on the southern campus where there were significantly more females than males. The majority of students were under 26 years of age; 213 students were under 18 and 584 between 18 and 25. The remaining 87 students were mature aged (> 25 years of age). Most of the students were enrolled at University on a full time basis (811) and 59 were enrolled on a part-time basis. Thirteen students did not respond to this question and one participant was auditing the course and therefore was not formally enrolled. Similarly, most of the students were either not employed (257) or employed on a part-time basis (533). Sixty-five were full-time employees, while 29 students did not respond to this question. The majority of students had used computers for more than 5 years; 480 had used computers between 6-10 years and 252 for longer than 10 years. Only 25 students had used computers for less than 2 years, while 126 had used computers between 3 and 5 years. One student did not respond to this question.

Students were asked to indicate what they used computers for. Table 2 provides relevant details. More than 80% of students indicated their main use was for Internet, e-mail and home use. Bank and work use formed a second grouping between 47%-50% and other areas of use (eg study and research; entertainment including games; and online purchasing and selling) accounted for 15.2%. Personal e-mail use was most prevalent (82.6%), followed by University use (81.2%) and Work-related use (24.7%).

Table 2: Participant Computer and e-Mail Usage

Variable	Category	Southern		Central		Northern		Total	
Computer Use	Home	380	81.9%	152	85.4%	190	78.5%	722	81.7%
	Work	208	44.8%	86	48.3%	124	51.2%	418	47.3%
	Banking	235	50.6%	98	55.1%	111	45.9%	444	50.2%
	e-Mail	412	88.8%	161	90.4%	214	88.4%	787	89.0%
	Internet access	415	89.4%	159	89.3%	218	90.1%	792	89.6%
	Other	63	13.6%	24	13.5%	46	19.0%	134	15.0%
	No response	2	0.4%	1	0.6%	1	0.4%	4	0.5%
E-Mail Use	Personal	387	83.4%	146	82.0%	198	81.8%	731	82.7%
	Work	111	23.9%	50	28.1%	57	23.6%	218	24.7%
	University	381	82.3%	144	80.9%	193	79.8%	719	81.3%
	Other	12	2.4%	5	3.4%	8	3.3%	26	2.9%
	No response	3	0.9%	1	0.6%	1	0.4%	6	0.7%
Participant	Totals:	464	NA	178	NA	242	NA	844	NA

Percentages have been calculated on the number of participants and may exceed 100.

Table 3 shows details of participant practices relating to e-mail access. The majority of students had either 2 or 3 e-mail accounts; 49.4% had 2 and 27.9% had 3. The remaining students had either one account (11.7%), or they had 4 or more e-mail accounts (11.0%). Almost 50% of the students access their e-mail at least once a day, with another 27.7% accessing several times a week. Sixty-one students did not respond to this question.

Table 3 also provides relevant details about password sharing and composition, specifically those associated with their e-mail accounts and other applications. Over half of the students used the same password (24.9%) or a slight variation of that password (31.2%). More than one-third of the students used passwords that were very different (36.3%). Sixty-seven students (7.6%) did not respond to this question. The participants were also asked whether they used other applications that required the use of passwords. Approximately 60% use passwords for other applications. There were three predominant groups: banking, other University applications and communication applications such as chat rooms, messenger services and forums. When asked whether they shared the same passwords across other applications, 37.5 % used the same password (17.4%) or a slight variation (20.1%). Approximately 40% of the students did not respond to this question.

Students were then asked questions concerning the composition and choice of their passwords – see Table 4. The majority of participants had passwords of greater than 5 characters in length. Participants typically used 8 characters in their password (29.2%), and 7.4% of the participants had passwords exceeding 11 characters. Approximately 39.4% of participants used only alphabetic characters in their passwords, while 42.2% used alphanumeric characters. The remaining students either used only numerals (6.4%); added symbols (4.1%); or did not respond to the question (7.5%). Typically their choice of password was meaningful data (43.1%) such as a name, street, preferred word, nickname, registration number and so on. A few selected pronounceable words (5.2%). Another 23.8% combined meaningful data items to make up their passwords. Only 10.7% choose a random combination of characters. Very few respondents had their passwords chosen for them (1.6%), while another 8% selected their password by some other means.

Table 3: Participant Practices Related to Accessing e-Mail and Sharing Passwords

Variable	Category	Southern		Central		Northern		Total	
Number of E-Mail Accounts	1 account	54	11.6%	31	17.4%	17	7.0%	102	11.5%
	2 accounts	243	52.4%	82	46.1%	112	46.3%	437	49.4%
	3 accounts	125	26.9%	44	24.7%	78	32.2%	247	27.9%
	> 4 accounts	42	9.1%	21	11.8%	35	14.5%	98	11.1%
Frequency Of Access	Several times a day	64	13.8%	41	23.0%	54	22.3%	159	18.0%
	Once a day	133	28.7%	62	34.8%	78	32.2%	272	30.8%
	Several times a week	144	31.0%	39	21.9%	62	25.6%	245	27.7%
	Once a week	63	13.6%	17	9.6%	23	9.5%	103	11.7%
	Several times a month	21	4.5%	8	4.5%	6	2.5%	36	4.1%
	Never check e-mail	5	1.1%	1	0.6%	2	0.8%	8	0.9%
	No response	34	7.3%	10	5.6%	17	7.0%	61	6.9%
Password Sharing Across E-Mail Accounts	Same password	110	23.7%	42	23.6%	68	28.1%	220	24.9%
	Slightly different	154	33.2%	52	29.2%	70	28.9%	276	31.2%
	No similarities	162	34.9%	62	34.8%	97	40.1%	321	36.3%
	No response	38	8.2%	22	12.4%	7	2.9%	67	7.6%
Password Sharing Across Applications	Same password	83	17.9%	31	17.4%	40	16.5%	154	17.4%
	Slightly different	100	21.6%	38	21.3%	40	16.5%	178	20.1%
	No similarities	96	20.7%	41	23.0%	57	23.6%	194	21.9%
	No response	185	39.9%	68	38.2%	105	43.4%	358	40.5%

Table 4: Participant Practices Relating to Password Composition

Variable	Category	Southern		Central		Northern		Total	
Password Length	1-5 characters	17	3.7%	5	2.8%	9	3.7%	31	3.5%
	6 characters	70	15.1%	20	11.2%	37	15.3%	126	14.3%
	7 characters	49	10.6%	21	11.8%	22	9.1%	93	10.5%
	8 characters	132	28.4%	56	31.5%	70	28.9%	258	29.2%
	9 characters	54	11.6%	18	10.1%	32	13.2%	104	11.8%
	10-11 characters	56	12.1%	20	11.2%	26	10.7%	102	11.5%
	> 11 characters	30	6.5%	17	9.6%	18	7.4%	65	7.4%
	No response	56	12.1%	21	11.8%	28	11.6%	105	11.9%
	Average	8.3		8.5		8.3		8.3	
	Minimum	1		3		1		1	
	Maximum	25		17		23		25	
Password Composition	Alphabetic only	197	42.5%	62	34.8%	89	36.8%	348	39.4%
	Numeric only	35	7.5%	5	2.8%	17	7.0%	57	6.4%
	Alphanumeric	176	37.9%	90	50.6%	108	44.6%	374	42.3%
	Includes symbols	22	4.7%	7	3.9%	7	2.9%	36	4.1%
	Other	1	0.2%	2	1.1%	0	36.8%	3	0.3%
	No response	33	7.1%	12	6.7%	21	8.7%	66	7.5%
Choice of Password	Meaningful data	207	44.6%	75	42.1%	99	40.9%	381	43.1%
	Combo meaningful data	109	23.5%	39	21.9%	62	25.6%	210	23.8%
	Pronounceable word	20	4.3%	10	5.6%	16	6.6%	46	5.2%
	Random characters	52	11.2%	17	9.6%	26	10.7%	95	10.7%
	Not self-chosen	6	1.3%	4	2.2%	4	1.7%	14	1.6%
	Other	35	7.5%	19	10.7%	17	40.9%	71	8.0%
	No response	35	7.5%	14	7.9%	18	7.4%	67	7.6%

E-mail accounts are heavily used as shown in Table 3 since at least 80% of students check their e-mail one or more times a day. This result could well be expected given that the participants in this study were students and e-mail communication is an essential aspect of their university study. What is of concern is the reuse of exact or similar passwords for different e-mail accounts and other applications (Table 4). Of the students responding to these two questions, 374 used the exact same password, 454 had passwords with a slight variation and 515 used completely different passwords. One promising factor was that half of the passwords were a combination of alphabetic, numerical and symbol characters and was on average 8 characters in length (Table 4). An interesting point is that only 14 participants had their passwords chosen by another entity such as their e-mail provider. All other passwords were self-selected, notwithstanding the 67 participants who did not respond to the question. With the exception of 31 students whose passwords were fewer than 6 characters long, password length ranged between 6 and 25 characters. Further, 60% of respondents had passwords of 8 or more characters in length. However, while this result is positive, the fact that almost three-quarters of the passwords contained meaningful detail, a combination of meaningful details or pronounceable words reduces its impact.

This outcome coupled with the fact that respectively, 61.9% and 19.8% of respondents never changed their password or changed it no more than three times a year, indicates a serious lack of concern with password security. Overall, respondents appear to be unconcerned about the risks associated with poor password composition. It would appear there is a need for a better education process on password composition for users. The education process should also focus on the wide variety of programs able to crack passwords relatively easily. It appears that while most respondents are aware of at least one of these types of programs, they fail to see the risks involved.

Table 5: Participant Practices Relating to Password Security and Management

Variable	Category	Southern		Central		Northern		Total	
Hand-written Record of Password	Wallet	10	2.2%	2	1.1%	5	2.1%	17	1.9%
	Diary	25	5.4%	15	8.4%	10	4.1%	50	5.7%
	Notebook	12	2.6%	5	2.8%	7	2.9%	24	2.7%
	Textbook	1	0.2%	3	1.7%	0	0.0%	4	0.5%
	Desk	9	1.9%	7	3.9%	3	1.2%	19	2.1%
	Drawer	13	2.8%	4	2.2%	6	2.5%	23	2.6%
	On PC Keyboard	2	0.4%	3	1.7%	1	0.4%	6	0.7%
	On PC Monitor	3	0.6%	1	0.6%	1	0.4%	5	0.6%
	Other	4	0.9%	2	1.1%	1	0.4%	7	0.8%
	No written copy kept	355	76.5%	133	74.7%	189	78.1%	677	76.6%
	Did not respond	39	8.4%	18	10.1%	21	8.7%	78	8.8%
Electronic Copy of Password	Mobile phone	17	3.7%	15	8.4%	11	4.5%	43	4.9%
	Electronic organiser	6	1.3%	0	0.0%	3	1.2%	9	1.0%
	USB device	4	0.9%	1	0.6%	1	0.4%	6	0.7%
	Computer disk	2	0.4%	1	0.6%	5	2.1%	8	0.9%
	File on hard drive	6	1.3%	4	2.2%	5	2.1%	15	1.7%
	File on shared network	1	0.2%	1	0.6%	0	0.0%	2	0.2%
	Other	1	0.2%	0	0.0%	0	0.0%	1	0.1%
	No electronic copy kept	375	80.8%	141	79.2%	197	81.4%	713	80.7%
	Did not respond	53	11.4%	19	10.7%	26	10.7%	98	11.1%
Frequency of Changing Password	Never	298	64.2%	105	59.0%	144	59.5%	547	61.9%
	< once a year	53	11.4%	25	14.0%	41	16.9%	119	13.5%
	1-3 times a year	33	7.1%	16	9.0%	7	2.9%	56	6.3%
	4-6 times a year	36	7.8%	14	7.9%	29	12.0%	79	8.9%
	Once a month	6	1.3%	1	0.6%	3	1.2%	10	1.1%
	Several time a month	3	0.6%	2	1.1%	1	0.4%	6	0.7%
	Did not respond	35	7.5%	15	8.4%	17	7.0%	67	13.5%
Sharing Passwords With Others	No other person	265	57.1%	102	57.3%	146	60.3%	514	58.1%
	A sibling	42	9.1%	15	8.4%	18	7.4%	75	8.5%
	A parent	23	5.0%	8	4.5%	6	2.5%	37	4.2%
	A partner/spouse	69	14.9%	23	12.9%	42	17.4%	133	15.0%
	Other relative	7	1.5%	3	1.7%	2	0.8%	12	1.4%
	Close friend	59	12.7%	30	16.9%	22	9.1%	111	12.6%
	Colleague	7	1.5%	1	0.6%	4	1.7%	12	1.4%
	Other	5	1.1%	0	0.0%	3	1.2%	8	0.9%
	Did not respond	37	8.0%	16	9.0%	18	7.4%	71	8.0%
Awareness of Passwords Cracking Techniques	Worm	154	33.2%	74	41.6%	88	36.4%	316	35.7%
	Virus	166	35.8%	79	44.4%	90	37.2%	335	37.9%
	Program file	100	21.6%	50	28.1%	61	25.2%	211	23.9%
	Other	16	3.4%	13	2.8%	20	4.3%	49	5.5%
	Did not respond	152	32.8%	51	28.7%	63	26.0%	266	30.1%

Respondents were also asked about sharing and remembering their passwords. Almost 60% of respondents (514) said they had not shared their password. Of the participants who had shared, most disclosure occurred with a family member (29.1%) while the remainder had shared their password with non-family members such as a close friend or colleague (14.9%). Respondents were divided with respect to admitting whether they had forgotten their password – 60.9% said they had not forgotten it compared to 30.4% who had; 8.7% chose not to answer this question. Respondents were also questioned whether they keep written versions of their passwords either in electronic or hard copy format. As shown in Table 5, many storage options were cited. However, over 76% of respondents said they did not keep copies of their password. It would appear that, for the most part, respondents are reacting positively towards messages about password practices of sharing and remembering.

CONCLUSION

This study has explored aspects of user password management practice within the context of e-mail usage by profiling e-mail account usage and password security practice. The results from this study provide important insight into on ongoing issues relating to the creation and management of user-based password management systems. The survey results support our initial focus on email account management as an important end-user application context. Email usage was very high with almost half of the participants using two e-mail accounts with a further two-fifths of all respondents using three or more email accounts. As anticipated, this creates password management difficulties for users and encourages password reuse across different email accounts, or their storage on paper and/or an electronic device for ease-of-reference. The poor password composition practices adopted by many of the respondents further compound this situation. Our results show that the vast majority of users are choosing passwords that are based on meaningful personal details that can be more readily guessed by others. While there have been significant technological developments in online authentication methods especially in graphics-based approaches (see for example Man et al. 2004 and Wiedenbeck et al. 2005), the password practices of users is an area that remains under researched. The results of this expanded study show that on the whole, the majority of users do not adopt secure management practices which in turn expose organisations to higher levels of risk and potential breaches in security. Future research will build upon this understanding and aim to gain further insight into how user practices can be improved. This knowledge can then be used as a basis for educational programs that focus on secure password practices.

REFERENCES

Adams, A. and Sasse, M.A. (1999) Users Are Not the Enemy, *Communications of the ACM*, 42:12, 41-46.

Bälter, O. (2000) How to Replace an Old Email System With a New, *Interacting with Computers*, 12:6, 601-614.

Carstens, D.S., McCauley-Bell, P., Malone, L.C. and DeMara, R.F. (2004) Evaluation of the Human Impact of Password Authentication Practices on Information Security, *Informing Science Journal*, 7:1, 67 – 85.

Conklin, A., Dietrich, G. and Walz, D., (2004) Password-Based Authentication: A System Perspective, *Proceedings of the 37th Hawaii International Conference on System Sciences*.

Furnell, S.M., Dowland, P.S., Illingworth, H.M. and Reynolds, P.L. (2000) Authentication and Supervision: A Survey of User Attitudes, *Computers & Security*, 19:6, 529-539.

Ives, B., Walsh, K.R. and Schneider, H. (2004) The Domino Effect of Password Reuse, *Communications of the ACM*, 47:4, 75-78.

Sherman, R. (1992) Biometrics Futures, *Computers & Security*, 11:2: 128-133.

Jobusch, D.L. and Oldehoeft, A.E. (1989) A Survey of Password Mechanisms: Part 1, *Computers & Security*, 8:7, 587-604.

Klein, D. (1990) A Survey of, and Improvements to, Password Security, *Proceedings of the USENIX Second Security Workshop*, Portland, Oregon, August 1990: 5-14.

Lee, A.S. (1994) Electronic Mail as a Medium for Rich Communication: An Empirical Investigation Using Hermeneutic Interpretation, *MIS Quarterly*, 18:2, June, 143-157.

Man, S., Hong, D., Hayes, B. and Matthews, M. (2004) A Password Scheme Strongly Resistant to Spyware, *Proceedings International Conference on Security and Management*, Las Vegas, 94-100.

Markus, M.L. (1994) Electronic Mail as the Medium of Managerial Choice, *Organization Science*, 5:4, November, 502-527.

Morris, R. and Thompson, K. (1979) Password Security: A Case History, *Communications of the ACM*, 22:11, 594-577.

Oppliger, R. (1997) Internet Security: Firewalls and Beyond, *Communications of the ACM*, 40:5, 92-105.

Rudy, I.A. (1996) A Critical Review on Research on Electronic Mail, *European Journal of Information Systems*, 4, 198-213.

Spafford, E.H., (1992) Opus: Preventing Weak Password Choices, *Computers & Security*, 11:3: 273-278.

Weber, R. (1999) *Information Systems Control and Audit*, Upper Saddle River, NJ: Prentice-Hall.

Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A. and Memon, N. (2005) PassPoints: Design and longitudinal evaluation of a graphical password system, *International Journal of Human-Computer Studies*, 63 102-127.

Zviran, M. and Haga, W.J., (1999) Password Security: An Empirical Study, *Journal of Management Information Systems*, 15:4, 161-185.

COPYRIGHT