Password Authentication from a Human Factors Perspective: Results of a Survey among End-Users

Peter Hoonakker[1], Nis Bornoe[2] and Pascale Carayon[1, 3]
[1] Center for Quality and Productivity Improvement, [3] ISyE Department
University of Wisconsin-Madison, USA
[2] IT University, Copenhagen, Denmark

Considering that many organizations today are extremely dependent on information technology, computer and information security (CIS) has become a critical concern from a business viewpoint. CIS is concerned with protecting the confidentiality, integrity, accessible information, when using computer systems. Much research has been conducted on CIS in the past years. However, the attention has been primarily focused on technical problems and solutions. Only recently, the role of human factors in CIS has been recognized. End-user behavior can increase the vulnerability of computer and information systems. In this study, using a large questionnaire survey among end-users, we examine password behavior of end-users.

INTRODUCTION

There is relatively little known about Computer and Information Security (CIS) breaches, the number of people and companies affected and the costs associated with these breaches. Furthermore, we know little about contributing factors, the kind of deviations from the computer and information security rules and possible consequences of these deviations.

There is very little reliable information about the costs of security breaches to companies and end users and the number of people and companies affected. Most of the information is either anecdotic or stems from commercial surveys among companies and end users. For example, results of a recent study among 5000 *consumers* by Javelin Strategy & Research (Monahan, 2007) revealed that *identity fraud* (defined as access to personal account information that leads to fraud) affects nearly 5% of consumers, or nearly 10 million people in the USA per year, and on average costs more than $6,000 per victim. The total one-year cost of identity fraud in the United States was more than $55 billion in 2006 (Monahan, 2007). Contrary to belief, most data compromise (91%) still takes place through offline channels and not via the Internet (9%). Lost or stolen wallets, check books or credit cards continue to be the primary source of personal information theft when the victim can identify the source of data compromise (30%). Nevertheless, computer viruses, spyware or hackers account for 5% of all identity fraud cases; phishing for 3%; and online transactions for 0.3% (Monahan, 2007). Extrapolating this data, around 800,000 Americans per year suffer from identity fraud via the Internet and the associated costs are around $5 billion per year.

Some states n the U.S. have made it mandatory for organizations to disclose *data security breaches*, if personal information was, or is reasonably believed to have been acquired by an unauthorized person. Results of a National Survey on Data Security Breach Notification by the Ponemon Institute LLC (2006) in 2005, show that nearly 12% of the respondents reported that they had received notification of a data security breach in the last year, suggesting that more than 23 million adult Americans may have received a breach notification (Durrett, 2006).

Results of the 2006 CSI/FBI Computer Crime and Security Survey (Gordon, Loeb, Lucyshyn, & Richardson, 2006) among 616 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions and universities, show that 56% of respondents reported *unauthorized use* of computer systems.

It is difficult to estimate *the total costs* associated with CIS breaches. For example, some reports estimate the global costs (based on tangibles such as lost productivity, network down time, and expenses incurred to get rid of virus infections) to combat the effect of computer viruses to be more than $12 billion (D'Amico, 2000). However, most firms do not report breaches in security because of fear of negative publicity (Campbell, Gordon, Loeb, & Zhou, 2003; Computer Security Institute, 2007). For example, in a study examining the economic effect of information security breaches reported in newspapers on publicly traded U.S. corporations, Campbell et al. (2003) found a highly significant negative stock market reaction for information breaches involving unauthorized access to confidential data.

The most reliable estimate of computer security breaches is based on the CSI/FBI Computer Crime and Security Survey. Results of the survey show that the average losses per company participating in their survey, was nearly $350,000 (Computer Security Institute, 2007).

To summarize: Computer and Information Security (CIS) has become an important concern from a business and personal viewpoint. However, we know relatively little about CIS, and especially from a human factors point of view.

In our study we collect information on non-malicious CIS deviations (defined as "breaking the rules" without malicious intent) by end users and possible reasons for these deviations. This research can help identify solutions for improving CIS-related behaviors of end users (i.e. reducing the occurrence of deviations or mitigating their impact on CIS). The focus in this paper is on computer authentication and how it can make computer and information systems more vulnerable.

BACKGROUNDS

The cheapest and most common used method of computer authentication is the use of usernames and passwords. Estimates show that 86% of U.S. companies use password authentication (Zhang, Luo, Akkaladevi, & Ziegelmayer, 2009). Alphanumeric passwords are used to protect both low and high sensitive information even though several major problems with alphanumeric passwords have been identified. Adams and Sasse (1999) concluded that four or five passwords are the most a typical user can be expected to use effectively. The human capacity for information processing is limited (Cowan, Morey, Gilchrist, & Saults, 2008 p. 50). As a consequence, users are having problems remembering their passwords and more importantly, to memorize and ***correctly match*** numerous passwords (Zhang, et al., 2009). This causes users to either use an easy password that is easy to remember but also easy to guess or to crack (Klein, 1990), or to use complicated passwords that are hard to guess or compromise but are difficult to remember.

Several studies have concluded that users in general create easy to remember and predictable passwords (Adams & Sasse, 1999; Schneier, 2006). Problems with weak passwords are not a new problem. In 1979, Morris & Thompson (1979) reported that many UNIX-users choose very weak passwords, for example very short or obvious passwords. They analyzed 3289 passwords and results showed that passwords mainly consisted of: strings of three ASCII characters (14%); strings of 4 alphamerics (a set of characters, including letters, numbers, and, often, special characters, such as punctuation marks) (15%); 5 letters, all upper-case or all lower case (21%) or 6 letters, all lower case (18%). Furthermore, 15% of the passwords appeared in various available dictionaries, etc. They concluded that a total of 86% of all passwords fitted in one the classes above. Ten years later Feldmeier et al. (1989) examined passwords and concluded that weak passwords along with password dictionaries continued to be a problem. Almost identical problems with weak passwords are seen today. Schneier (2006) examined 34,000 MySpace usernames and passwords. Results showed that 65% of all passwords contained 8 characters or less. The most frequently used password were: password1; abc123; myspace1; and password (Schneier, 2006).

Users can use several work-arounds to overcome their limitations: using the same password for every system they access, writing down passwords, storing passwords in electronic files, and reusing or recycling old passwords (e.g. password2007 becomes password2008). Users seem to use all strategies. For example, according to Horowitz (2001), 15–20% of the users of an office supply manufacturer on a regular basis wrote down their password on a post-it sticker next to their computer. Results of a study among 1300 business professionals show that 66% of respondents reported that employees keep password paper records at work and 58% reported that employees keep electronic password records (for example in a Word document or spreadsheet) (Bedford, 2006). It is also common to reuse passwords. Results of a survey by Brown et al. (2004) showed that nearly all participants reused passwords. Overall, 82% of end users are frustrated with managing passwords at work (Bedford, 2006).

In this study we examine password behavior of end-users; whether password behavior is related to CIS vulnerability; and whether end-users beliefs and attitudes towards CIS are related to password behavior and vulnerability.

METHODS

Focus Groups

Because relatively little is known about Computer and Information Security (CIS) behavior of end-users, we first conducted focus groups with network administrators and CIS experts Hoonakker et al. (2008). A focus group interview is defined as an interview with a small group of people on a specific topic. Two rounds of focus groups interviews were conducted with the two different groups (CIS experts and network administrators). During the first focus group interview, participants were asked to describe non-malicious CIS deviations, and elaborate on contributing factors and possible consequences. During the second round of focus groups, we gave feedback on the results of the first focus group and tried to reach a consensus on the most important deviations from the security rules. The focus groups were conducted over the phone, consisted of 5-7 participants and lasted each one-and-a-half hour. The focus groups were audio taped and transcribed into anonymized text files. The text files were analyzed using qualitative data analysis software.

Questionnaire Survey

Based on the results of the focus groups, we developed a survey questionnaire to measure end-users' deviations from the rules and possible contributing factors to these deviations. Analysis of the focus group data resulted in 10 major areas that are related to CIS deviations: 1) Accessing the computer system and password; 2) Security settings of the computer; 3) System maintenance and downloading software; 4) Electronic mail; 5) Help with computer problems; 6) Remote access and working from home; 7) Sharing the computer and social networking; 8) CIS training; 9) CIS policy; and 10) Beliefs and attitudes towards CIS. In this paper we focus on the results with regard to computer authentication.

Sample

A representative sample of employees of a large organization was asked to fill out a web-based survey. The organization handles very sensitive private information and has experienced computer security problems in the past. A Computer and Information Security training is mandatory for all employees at the organization.

Totally 836 employees filled out the questionnaire (53% response rate). Seventy percent of the respondents are female. Average age is 50 years. On an average, respondents have 18.2 years of computer experience. Three percent of

respondents categorize themselves as novice users (just started using computers); 69% as average users (use word processors, spreadsheets, e-mail, surf the Web, etc.); 22% as advanced users (can install software, setup configurations, etc.); and 6% as expert users (can setup operating systems; know some computer programming languages, etc.). Respondents had varying educational backgrounds: high school or GED (8%); some college (14%); 2-year college (14%); 4-year college (37%); Master's degree (MA, MS: 21%); professional degree (MD, JD: 3%); and doctoral degree (PhD: 3%). On an average, respondents have worked more than 14 years for the organization. Ninety-five percent of the respondents are normal end-users; 3% super-users (have some administrator rights); and 2% network administrators.

RESULTS

The results of the questions on password use are summarized in Table 1.

Table 1: Password use practices

1	On an average, respondents have different 4.1 passwords to logon to different computers and/or access different computer applications at work. If we include passwords used at home that number increases to 9.
2	Eighteen percent of the respondents always use the same password to access the different computer systems, application or websites, 50% sometimes use the same password and sometimes another password, and 31% always use different passwords.
3	Sixty-three percent of the respondents who use more than one password make a difference between systems that need special protection (e.g. their office network) and systems for which they can use an easy to use and remember password.
4	On an average, respondents change their password 7 times a year, almost always prompted (96%) by their department.
5a	Fifty-six percent of the respondents use a long password (more than 8 characters);
5b	Seventy-nine percent use a combination of upper and lower cases and;
5c	Thirty-eight percent use special characters (e.g. #,*,^) when they change their password.
6	When they change their password, 68% of the respondents re-use their old password (e.g. password2007 becomes password2008).
7	Fifty-six percent of respondents write their passwords down.
8	Seven percent of respondents keep their username-/passwords in an electronic file (e.g. Word document).
9	Eighteen percent of the respondents who keep their password in an electronic file secure the electronic file(s) by password protecting or encrypting it.
10	One percent of respondents uses software to keep track of their passwords (e.g. Internet Explorer password manager, , Password manager, Roboform, etc).
11	Five percent of respondents share their password(s) with other people.
12	Thirty-eight percent of respondents use a password protected screensaver.
13	Seventy-nine percent of respondents use a screen lock. For example, they use Windows Lock Workstation option, meaning that they have to login again when they have left their computer and come back, using CTRL-ALT-DEL.
14	Thirty percent of respondents always log off when they step away from their computer.
15	Eighty-five percent of respondents always turn off their computer when they are done for the day.

When we select the respondents who ***deviate*** from Computer and Information Security (CIS) best practices with respect to password use, that is, the respondents who: always use only one password to access the different systems (1 and 2); who use a password shorter than or equal to 8 characters, do not use a combination of upper and lower cases or do not use special characters (5a, 5b, 5c); do re-use their old passwords (6); do write down their passwords (7); keep their passwords in an electronic file without protecting it (8 and 9) or who share passwords with other people, and analyze the data, results show that only 4% of the respondents do ***not*** deviate from the best practices with regard to password use, and that the other 94% do deviate from one or more best practices (see Table 2).

Table 2: Number of deviations from best password practices

Deviations	N	Percent of total
0	37	4.4%
1	111	13.3%
2	224	26.8%
3	250	29.9%
4	163	19.5%
5	53	5.1%
6	8	1.0%
Total	836	100%

On an average, respondents deviate 2.7 times from best practices for password use. If we include best practices with regard to leaving the computer unattended at the work place (#13-#15 in Table 1: respondents who do not use a screen lock, who do not always log off when they step away from the computer or do not turn off the computer when they are done for the day), and analyze the results again, results show that only 2% of the respondents do not deviate from the best practices.

Results of statistical analysis show that user type (novice, average, advanced or expert user) is the strongest factor related to the number of deviations. Gender, age, education, job position the organizational unit the respondents work in, and years of computer experience, are less important. For example, results of our analyses show that network administrators and super-users perform slightly better than normal end-users in the number of deviations from the password best practices, but the differences are not

statistically significant (χ^2=20.2, *df*=12, p=0.06). Expert users and to a lesser extent advanced users perform significantly better than average users and novice users. For example, 15% of expert users, 7% of advanced users, 2% of average users and 7% of novice users do *not* deviate at all from the best practices (χ^2=48.1, *df*=18, p<0.01). An example of the differences between different users and password practices is shown in Figure 1: password use (always same password, sometimes the same and sometimes different passwords, or always different passwords) by user type.

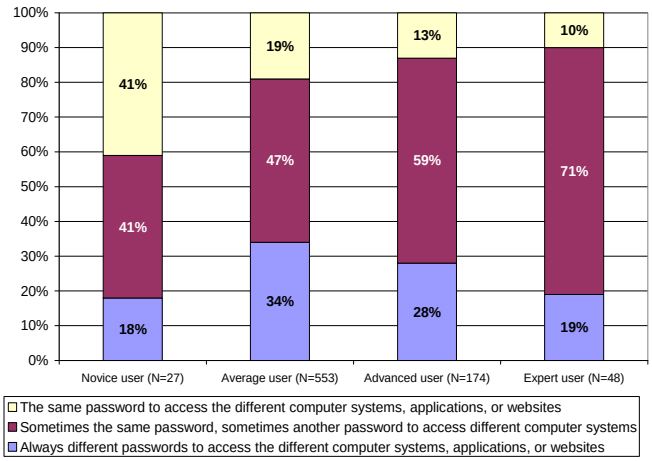

Figure 1: Password use by user type

We examined the relation between attitudes about computer and information security (CIS) and password use. Results of a clusters analysis show that a minority of the respondents (7%) are cynical about efforts to protect their computers from harm (for example, they disagree with the statement: "I can protect my computer from harm (hackers, phishing, etc.) if I take good care of computer security (change passwords on a regular basis, use firewalls, encryption, etc.)". Fourteen percent do not know what to think (neither agree nor disagree), but the majority (77%) do believe that it makes a difference. Interestingly, there are no differences in the number of deviations from best practices for password use. The "cynical" respondents deviate on an average 2.6 from best practices, the "do not know group" on an average 2.8, and the "believers" deviate on an average 2.6 times from best practices.

CONCLUSIONS

Much of the attention in the past to improve Computer and Information Security (CIS) has been focused on hardware and software solutions. Relatively little attention has been paid to "peopleware". However, several studies have shown that humans and the way they interact with computer systems are the weakest link in CIS. To quote Mitnick and Simon (2002): "A company may have purchased the best security technologies that money can buy, trained their people so well that they lock up all their secrets before going home at night, and hired building guards from the best security firm in the business. The company is still totally vulnerable... The human factor is truly security's weakest link".

The use of alphanumeric usernames and passwords is the most often used (and also the cheapest) method of computer authentication. However, unfortunately human beings are limited in their information processing capabilities (Cowan, et al., 2008). People either use simple passwords that are easy to remember but easy to crack or difficult passwords which are difficult to remember. Results of our study have shown that there are very few people who do not deviate from the best practices for password use. Respondents either use the same password all the time, or use relatively simple passwords; respondents re-use their old password; write passwords down; either on paper or store it in an electronic file without protecting it; respondents share passwords, etc. In reality, the results are probably worse, because respondents do not like to admit that they deviate from the rules. Results also show that respondents who believe that it matters to pay attention to CIS deviate as often from best practices for password use as people who are cynical about CIS. These results indicate that it is not so much unwillingness of the end-users to adhere to the rules, but that they are not capable of "sticking to the rules". Results of a study by Zhang et al (2009) showed that interference caused by having to use a series of passwords for the same account, or interference between different password-protected accounts is one of the most important reasons for multiple password recall errors, and is one of the most frustrating aspects of password authentication system for users.

In deviating from the best practices, end-users can make the best protected computer systems vulnerable. Problems with the use of alphanumeric passwords have been known for more than 20 years, but unfortunately, so far we have made little progress (Ives, Walsh, & Schneider, 2004).

A possible method to improve password security is to use mnemonic techniques such as using the first letters of a relatively easy to remember phrase or sentence as a password (e.g. "star paliblic dash bang" becomes: "*paliblic-!"). The literature shows that passwords created this way are more difficult to crack than textual passwords (Kuo, Romanosky, & Cranor, 2006). There are websites that generate such passwords. However, using passwords that are more difficult to crack does not make them easier to remember,

There are also other solutions to overcome human limitations. For example several studies have shown that human beings are better at recognizing pictures than words or sentences (Shepard, 1967) and pictures are better stored in the long-term memory . Humans do not seem to have a specific limit regarding how many pictures can be stored in long term memory and pictures are easily remembered (Haber, 1970). Studies have shown that picture based passwords have a better memorability than alpha-numeric passwords and PIN numbers (Dhamija & Perrig, 2000). Graphical passwords are not a security "silver bullet", but a possible alternative for usable yet secure authentication. Other, but more expensive solutions are token-based or smart card authentication, or the use of biometrics (fingerprints, retinal scan, etc.). However, even these more expensive systems are not bullet-proof (O'Gorman, 2003).

Most efficient are two- or three step authentication methods, for example a combination of a token based ands knowledge-based authentication (for example a smart card in combination with a PIN number), a combination of biometrics and passwords, or a combination of token-based authentication and biometrics, depending on the level of security needed (O'Gorman, 2003).

In the future, a better balance has to be found between the limitations of human beings and the desire for increased security. Several studies have pointed out the potential conflict between usability and security (Furnell, 2005; Renaud, 2005; Weir, Douglas, Carruthers, & Jack, 2009). Two- or three factor authentication is probably the most promising approach. However, also in two- or three factor authentication approaches, usability plays a crucial, if not a more important role. For example, in an interesting, recent study, Weir et al. (2009) compared three two-factors authentication methods for eBanking on security and usability. Results of the study show that two thirds of participants preferred the device that they perceived the least secure, but most user-friendly (Weir, et al., 2009). Thus, in the future, more research on how perceptions of usability, security, and convenience are related, are needed. Perceived usefulness, ease of use and user satisfaction determine (correct) use of technology, not the other way around (Davis, 1989).

ACKNOWLEDGEMENTS

This study was made possible with a grant from the National Science Foundation. Grant number: CNS-0627682 (PI: Pascale Carayon).

REFERENCES

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM, 42*(12), 41-46.

Bedford, M. A. (2006). RSA Security Research Shows Volume of Business Passwords Overwhelming End Users and Hindering IT Security Efforts. *RSA Press Releases* Retrieved May 26, 2009, from http://www.rsa.com/press_release.aspx?id=7296

Brown, A. S., Bracken, E., Zoccoli, S., & Douglas, K. (2004). Generating and remembering passwords. *Applied Cognitive Psychology, 18*(6), 641-651.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security, 11*(3), 431.

Computer Security Institute (2007). *2007 CSI Computer Crime and Security Survey*. San Francisco, CA: Computer Security Institute.

Cowan, N., Morey, C. C., Chen, Z., , Gilchrist, A. L., & Saults, J. S. (2008). Theory and measurement of working memory capacity limits. In B. H. Ross (Ed.), *The Psychology of Learning and Motivation* (Vol. 49, pp. 49-104). Amsterdam: Elsevier B.V.

D'Amico, A. D. D. (2000). *What Does a Computer Security Breach Really Cost?* Northport NY: Secure Decisions.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319-340.

Dhamija, R., & Perrig, A. (2000). *Déjà vu: A user study using images for authentication.* Paper presented at the 9th Conference on USENIX Security Symposium, Denver, CO.

Durrett, D. M. (2006). *The Costs of Data Security Breaches and Identity Theft*. Cary, NC: Covelight Systems.

Feldmeier, D. C., & Karn, P. R. (1989). UNIX Password Security - Ten Years Later. *Computer Science, 435*, 44-63.

Furnell, S. (2005). Why users cannot use security. *Computers & Security, 24*, 274-279.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2006). *2006 CSI/FBI Computer Crime and Security Survey* (No. 8). San Francisco, CA: Computer Security Institute.

Haber, R. N. (1970). How we remember what we see. *Scientific American, 222*(5), 104-112.

Hoonakker, P. L. T., Carayon, P., Deb, J., El Desoki, R., & Veeramani, R. (2008). The use of focus groups to examine human factors in computer and information security. In L. I. Sznelwar, F. L. Mascia & U. B. Montedo (Eds.), *Human Factors in Organizational Design and Management - IX* (pp. 377-382). Santa Monica, CA: IEA Press.

Horowitz, A. (2001). Top 10 Security Mistakes. *Computerworld* Retrieved Nov 13, 2008, from http://www.computerworld.com/securitytopics/security/story/0,10801,61986,00.html

Ives, B., Walsh, K. R., & Schneider, H. (2004). The domino effect of password reuse. *Communications of the ACM, 47*(4), 75-78.

Klein, D. V. (1990). *Foiling the cracker: a survey of, and improvements to, password security.* Paper presented at the 2nd USENIX Workshop Security.

Kuo, C., Romanosky, S., & Cranor, L. F. (2006). *Human Selection of Mnemonic Phrase-based Passwords.* Paper presented at the Second symposium on Usable privacy and security, Pittsburgh, PE.

Mitnick, K. D., & Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security*. New York, NY: John Wiley & Sons.

Monahan, M. T. (2007). *2007 Identity Fraud Survey Report: Identity Fraud Is Dropping, Continued Vigilance Necessary*. Pleasanton, CA: Javelin Strategy & Research.

Morris, R., & Thompson, K. (1979). Password Security: A Case History. *Communications of the ACM, 22*(11), 594-597.

O'Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE, 91*(12), 2021-2040.

Ponemon Institute LLC (2006). *2006 Annual Study: Cost of a Data Breach*. Elk Rapids, MI: Ponemon Institute LLC.

Renaud, K. V. (2005). Evaluating Authentication Mechanisms. In L. Cranor & S. Garfinkel (Eds.), *Security and Usability*.

Schneier, B. (2006). MySpace Passwords Aren't So Dumb. *Wired* Retrieved Nov 12, 2008, from http://www.wired.com/politics/security/commentary/securitymatters/2006/12/72300

Shepard, R. N. (1967). Recognition memory for words, sentences, and pictures. *Journal of Verbal Learning and Verbal Behavior, 6*(1), 156-163.

Weir, C. S., Douglas, G., Carruthers, M., & Jack, M. (2009). User perceptions of security, convenience and usability for ebanking authentication tokens. *Computers & Security, 28*(1-2), 47-62.

Zhang, J., Luo, X., Akkaladevi, S., & Ziegelmayer, J. (2009). Improving multiple-password recall: an empirical study. *Eur J Inf Syst, 00*, 1-12.