The Effect of Educating Users on Passwords: a Preliminary Study

VIKTOR TANESKI, BOŠTJAN BRUMEN and MARJAN HERIČKO, University of Maribor

Passwords are a basic authentication method for most information systems. Despite their widespread use, passwords still suffer from a number of problems. Users and their passwords are the Achille's heel (the weakest link) of security, because they still tend to create passwords that are weak, easy to remember and contain words that a familiar to them. They also tend to trade security for memorability. Users' lack of security consciousness and their behaviour can be influenced by information security training. This paper presents the preliminary results of our research in progress. Our research explores the effect of password security training on strength of the passwords chosen by the users and their consciousness about security and the importance of creating strong and hard-to-guess passwords. We collected the data by means of an online questionnaire, performed among undergraduate students from the Faculty of electrical engineering and computer science at the University of Maribor. Overall, the results show that, despite our lectures and recommendations, users still lack of security knowledge regarding password change and password write-down and need to be further educated in this direction.

Categories and Subject Descriptors: K.3.2 [**Computers And Education**]: Computer and Information Science Education—*Accreditation, Computer science education, Curriculum, Information systems education, Literacy, Self-assessment*; K.4.0 [**Computers and Society**] General; K.6.5 [**Management Of Computing And Information Systems**]: Security and Protection—*Authentication, Unauthorized access*

General Terms: Human Factors, Security

Additional Key Words and Phrases: Authentication, computer security, passwords, password security, password security education

1. INTRODUCTION

Password-based authentication mechanisms are the primary means by which users gain legitimate access to a computer system. Although alternative authentication methods such as biometrics (based on "what you are"), smart cards (based on "what you have") and two-step verification are becoming more available, passwords remain the most common method for authentication for computer systems. But passwords suffer from a number of problems known for some time now. Password-related problems are firstly identified by Morris and Thompson [1979]. The authors conducted experiments in order to determine typical users' habits about the choice of passwords and noticed that users of the system chose passwords that are short, simple and contained only lowercase letters and digits, or appeared in various dictionaries. These findings were confirmed 20 years later by Zviran and Haga [1999]. The authors concluded that one of the biggest vulnerabilities to a computer system's security is the user. Almost 50

Author's address: V. Taneski, Faculty of electrical engineering and computer science, University of Maribor, Smetanova ul. 17, 2000 Maribor, Slovenia; email: viktor.taneski@um.si; B. Brumen, Faculty of electrical engineering and computer science, University of Maribor, Smetanova ul. 17, 2000 Maribor, Slovenia; email: bostjan.brumen@um.si; M. Heričko, Faculty of electrical engineering and computer science, University of Maribor, Smetanova ul. 17, 2000 Maribor, Slovenia; email: marjan.hericko@um.si.

In: Z. Budimac, T. Galinac Grbac (eds.): Proceedings of the 3rd Workshop on Software Quality, Analysis, Monitoring, Improvement, and Applications (SQAMIA), Lovran, Croatia, 19.-22.9.2014, published at http://ceur-ws.org.

percent of the users surveyed in the study reported passwords composed of five or fewer characters, 80 percent used only alphanumeric characters, and 80 percent never changed their password.

A recent literature review in the area of textual passwords and textual passwords security Taneski et al. [2014], summarises the most common problems related to creating and managing textual passwords. The review also summarises proposed solutions and approaches for better coping with the identified problems with textual passwords. Many approaches and solutions, for increasing the security and usability of textual passwords, were proposed through the years but none have proven widely acceptable. The review shows that, despite all these approaches, recommendations, security policies and etc., users still encounter the majority of the identified and already known problems. Users and their textual passwords are still considered "the weakest link", because they still tend to choose weak passwords and passwords that can be found in a dictionary [Egelman et al. 2013] and are likely to use words that are familiar to them as their passwords [Bishop and Klein 1995]. Because of the rapid growth of the popularity of Internet technology and the increased number of online services requiring password-based authentication, users have to maintain many different accounts and have to remember multiple passwords. This leads to users to frequently forget their passwords, write them down or share them with their friends [Jakobsson and Dhiman 2013]. Users create the easiest-to-remember passwords regardless to any recommendations or instructions and tend to trade security for memorability [Zviran and Haga 1990; Zviran and Haga J. 1993]. These problems can arise as a result of users' lack of security motivation and understanding of password policies and the fact that users tend to circumvent password restrictions for the sake of convenience [Adams et al. 1997]. This indicates a deficit in user's consciousness about security and this user behaviour can be influenced by information security training [Horcher and Tejay 2009]. Educating users about password security and the importance of creating strong and hard-to-guess passwords and assisting them with creating secure passwords can raise the security consciousness of system users and can help achieve greater security [Zviran and Haga 1999].

This study, which is research in progress, explores the recommendation of Zviran and Haga [1999] by analysing the effect of password security training on user's practices regarding password creation, password use and management and their consciousness about security and the importance of creating strong and hard to guess passwords. We performed a pilot study on university students about their password practices, attitudes and knowledge about password creation and password security. We administered the survey in two phases over one month period along with several lessons on password security between the two phases. The first phase of the survey was performed among students that had no password security training. The second phase of the survey was performed one month later on the same group of students. For a period of two weeks, between the two phases, the students were educated about the importance of password security and how to manage their passwords. Following the lectures there was a two week period for learning decay. The contribution of this study in this manner is that we succeeded in educating the participants about some password practices, in contrast to some previous studies Hart [2008], Dhamija and Perrig [2000] that have not proven to be successful at all. Finally, we present the preliminary results of our survey.

The rest of the paper is organized as follows: in Section 2 we describe the research method; in Section 3, we present the results of the survey and a discussion; Section 4 concludes the paper and presents plans for future work.

Table I. Questionnaire Categories

Category	**Description**
Account information	which services or devices does the student have a password for (desktop computer, notebook computer, mobile phone, tablet, University account, Facebook account, Twitter account, Google account)
Password information	the characteristics of the selected passwords (first character, length, how did the user choose the passwords etc.)
Password recall	how often do users forget their passwords, how often do they change them and how often do they write their passwords down
Frequency of password use	information about the frequency of password use (how often do users log in by using the password, and whether they use the password to log in to multiple accounts)
Data importance and data sensitivity	how important and how sensitive is to users the data that they are protecting
Demographic data about the user	gender, year of birth, university, faculty, postal code etc.

2. METHOD

2.1 The Survey

Data for this study is collected by means of an online questionnaire. The main objective of the questionnaire is to determine the characteristics of textual passwords used by individuals to log in, mainly to a university account, but also to other accounts, such as Facebook, Twitter, Google, or their own mobile devices and phones. Because asking users about their passwords is a sensitive topic, we did not ask about their actual passwords but about the characteristics of their passwords for different accounts. We classify the questions into six categories, presented in Table I.

For creating our questionnaire, we drew inspiration from the questionnaire that was performed by Zviran and Haga [1999]. Our questionnaire has additional questions and additional answer options about password characteristics for different accounts for different services or devices, thus allowing us to compare characteristics of different passwords for different accounts. The completion of the questionnaire took between 15 and 20 minutes.

2.2 Participants

A total of 33 undergraduate students from the Faculty of electrical engineering and computer science at the University of Maribor, participated and completed the first phase of the web-based survey. 30 of them also completed the second phase of the study, but 24 attended the lectures about password security. All of the participants were regular users of the Internet and modern mobile devices and smart phones, with one or more different password-protected accounts. Five participants were female and 28 male in the first phase, and three were female and 27 male in the second phase. The average age of the participants is 22.

2.3 Procedure

The survey was conducted in spring term 2014 and consisted of two phases. The first phase of the questionnaire was performed among students that did not receive the lessons. After the first phase of the survey, the students attended lectures dedicated specifically to passwords and related issues, like password creation, management and security. The education consisted of topics about the importance of creating strong and secure passwords, how to choose such passwords and how to manage them. After the education part followed a two week period of learning decay, followed by the second phase of the survey. We slightly modified the questionnaire by adding an additional answer option “I prefer not to disclose” to every question in the “Password information” section. By adding this answer option, we want to determine if the users that attended the lectures are more conscious about the importance of concealing information about their passwords.

Table II. Summary of Common Password Characteristics (Phase 1)

Account	Common password characteristics	Count	No answer
desktop computer	alphabetic - lowercase letters only (e.g. password)	5 (15.15%)	17 (51.52%)
notebook computer	alphabetic - lowercase letters only (e.g. password)	7 (21.21%)	4 (12.12%)
mobile phone	numeric - digits only (e.g. 12345)	13 (39.39%)	11 (33.33%)
tablet device	numeric - digits only (e.g. 12345)	2 (6.06%)	28 (84.85%)
University account	alphanumeric - single case letters and 1-2 digits behind (e.g. pass1, pass12, PASS1, PASS12)	9 (27.27%)	3 (9.09%)
Facebook account	alphanumeric - mixed case letters and 3 or more digits (e.g. Pass1W34oR9d)	7 (21.21%)	3 (9.09%)
Twitter account	alphanumeric - mixed case letters and 3 or more digits (e.g. Pass1W34oR9d)	4 (12.12%)	21 (63.64%)
Google account	alphanumeric - mixed case letters and 3 or more digits (e.g. Pass1W34oR9d)	7 (21.21%)	6 (18.18%)

Table III. Summary of Common Password Characteristics (Phase 2)

Account	Common password characteristics	Count	No answer
desktop computer	alphanumeric - mixed case letters and 1-2 somewhere (e.g. Pass12Word, Pa12ssWord, 1PassWord2)	5 (20.83%)	9 (37.50%)
notebook computer	alphanumeric - mixed case letters and 1-2 somewhere (e.g. Pass12Word, Pa12ssWord, 1PassWord2)	7 (29.17%)	2 (8.33%)
mobile phone	numeric - digits only (e.g. 12345)	9 (37.50%)	9 (37.50%)
tablet device	numeric - digits only (e.g. 12345)	1 (4.17%)	22 (91.67%)
	alphanumeric - single case letters and 1-2 digits in between (e.g. pass12word, PASS12WORD, P12ASSWORD)	1 (4.17%)	
University account	alphanumeric - single case letters and 1-2 digits behind (e.g. pass1, pass12, PASS1, PASS12)	5 (20.83%)	2 (8.33%)
Facebook account	alphanumeric - mixed case letters and 3 or more digits (e.g. Pass1W34oR9d)	4 (16.67%)	2 (8.33%)
	mixed case letters, several special characters and several digits (e.g. 3Pa!s45Wor$d)	4 (16.67%)	
Twitter account	alphanumeric - mixed case letters and 1-2 somewhere (e.g. Pass12Word, Pa12ssWord, 1PassWord2)	2 (8.33%)	16 (66.67%)
	alphanumeric - single case letters and 3 or more digits (e.g. 1PASS23WORD4, pass1wor3d4)	2 (8.33%)	
Google account	alphanumeric - mixed case letters and 1-2 somewhere (e.g. Pass12Word, Pa12ssWord, 1PassWord2)	4 (16.67%)	5 (20.83%)

3. RESULTS

We compared password characteristics of the user group before the users attended the password security lectures (phase 1) and after the lectures (phase 2). Thirty participants attended the second phase of the questionnaire, but not all of them (24) attended the lectures. We took in consideration only the participants that attended the lectures. In this section, we summarise the preliminary results of our study, by comparing the results from the two phases of the survey. We present the results about the general password characteristics (password length, password composition), password change frequency, and password memorability and write-down.

3.1 General Password Characteristics

While we ask our participants about their password characteristics, we do not inquire their actual passwords. The question that we ask in both phases is “What are the characteristics of your password?”. The answers to the question for both phases are summarised in Table II and Table III respectively. In both tables, the first column denotes the specific accounts, the second column represents the most common answers about password characteristics for every account, the third column represents the percentage od users who chose that answer. The last column of each table represents the number of

Table IV. Average Password Length

Account	Average password length		
	Phase 1	**Phase 2**	**Not disclosing**
desktop computer	8.81	10.77	2
notebook computer	8.79	11.00	4
mobile phone	4.91	6.08	2
tablet device	5.40	5.50	0
University account	7.67	8.70	2
Facebook account	10.33	12.06	4
Twitter account	9.00	10.33	2
Google account	10.48	12.59	2

participants that did not answer the question for the specific account (since there is a possibility that the user had not created that account). The results summarised in Table II show that the passwords for the desktop and notebook account consist of most commonly lowercase letters only, regardless the fact that 15.15% of the users rated their data on their desktop computer as very important, and 45.45% rated their data on their notebook computer, also as very important. The results in Table III demonstrate that the passwords for these accounts in the second phase of the study are mostly alphanumeric with mixed case letters and numbers. Thus, we can observe an improvement in the characteristics of the passwords for the desktop and notebook accounts. It is most likely that, after attending the lectures about passwords and password security, the awareness of users about the importance of their data and the importance of creating strong and hard to guess passwords for the data, increased. These findings are in line with the statement of Adams et al. [1997] that, users lack of security knowledge. Very often users are not conscious about the security and the importance of their data, and they need additional guidance on information importance and sensitivity.

In regard to the average password length, we provided lectures for the participants and gave them recommendations about the design, management and protection of strong and hard-to-guess passwords. The data about the average password length for both phases is summarised in Table IV. The first column denotes again the specific accounts, while the second and third columns represent the average password length for the first and second phase, respectively. The last column represents the number of participants in the second phase, that answered the specific question about the password length for their accounts with “I prefer not to disclose”. The results revealed an increased average password length in almost every account in the second phase of the study. One possible explanation for these findings may be that the increase of the average password length is a result of the users changing their passwords after attending the lectures.

3.2 Password Change Frequency

We trained the participants about the importance of frequent password change in order to ensure that a stolen password can not be used to compromise other passwords and accounts of other users in the system. The frequent password change is a basic security measure [Zviran and Haga 1999]. But, because of the rapid growth of the popularity of the Internet and the increased number of online accounts, a user has to maintain many different passwords [Notoatmodjo and Thomborson 2009]. Because of this, the forced and too frequent password changes can have negative effect on the users (users may quickly forget which password is current, which may lead to users tempting to write their passwords down or to reuse an old one) [Sasse et al. 2001]. The research in literature still supports frequent password changing to reduce predictability and suggests that a realistic time for password change for the average user may be 90-120 days [P. Cisar and Cisar 2007]. In the first phase, we asked our participants “How often do you change your password (when not required by the system)?”, and in

Table V. Frequency of Password Change (Phase 1)

Frequency	desktop comp.	notebook comp.	mobile phone	tablet device	University account	Facebook account	Twitter account	Google account
never changed it since first use	6 (18.18%)	7 (21.21%)	8 (24.24%)	2 (6.06%)	18 (54.55%)	6 (18.18%)	6 (18.18%)	7 (21.21%)
less than once a year	6 (18.18%)	12 (36.36%)	9 (27.27%)	2 (6.06%)	8 (24.24%)	12 (36.36%)	3 (9.09%)	8 (24.24%)
up to three times a year	3 (9.09%)	6 (18.18%)	2 (6.06%)	0 (0%)	2 (6.06%)	6 (18.18%)	1 (3.03%)	7 (21.21%)
four to six times a year	1 (3.03%)	3 (9.09%)	3 (9.09%)	1 (3.03%)	1 (3.03%)	5 (15.15%)	0 (0%)	3 (9.09%)
about once every month	0 (0%)	0 (0%)	1 (3.03%)	0 (0%)	0 (0%)	0 (0%)	1 (3.03%)	2 (6.06%)
more than once a month	0 (0%)	1 (3.03%)	0 (0%)	0 (0%)	1 (3.03%)	1 (3.03%)	1 (3.03%)	0 (0%)
No answer	17 (51.52%)	4 (12.12%)	10 (30.30%)	28 (84.85%)	3 (9.09%)	3 (9.09%)	21 (63.64%)	6 (18.18%)

Table VI. Password Write-down

Answer	Phase	desktop comp.	notebook comp.	mobile phone	tablet device	University account	Facebook account	Twitter account	Google account
Yes	First	2 (6.06%)	3 (9.09%)	2 (6.06%)	1 (3.03%)	6 (18.18%)	2 (6.06%)	1 (3.03%)	3 (9.09%)
	Second	1 (4.17%)	1 (4.17%)	1 (4.17%)	0 (0%)	5 (20.83%)	3 (12.50%)	0 (0%)	3 (12.50%)
No	First	13 (39.39%)	25 (76.76%)	20 (60.61%)	3 (9.09%)	23 (69.70%)	27 (81.82%)	10 (30.30%)	23 (69.70%)
	Second	12 (50%)	19 (79.17%)	13 (54.17%)	2 (8.33%)	16 (66.67%)	18 (75%)	8 (33.33%)	15 (62.50%)

the second phase, following the lectures, we asked them "whether they changed their password since the last survey or not, and why?". Table V summarises the result of the frequency of password change in the first phase of the study. We found that many users never change their password for the specific account since its first use, or rarely change it (less than once a year). Despite our lectures and recommendations, the results show that a large percent of the users (41.67% for the Facebook account, 37.50% for the Google account, 50% for the notebook computer and even 66.67% for the University account) did not change their password since the first phase of the study. Overwhelming and promising are the findings about the users who changed their passwords since the first phase and after attending the lectures. Even 25% for the desktop computer, 33.33% for the notebook computer, 20.83% for the University account, 29.17% for the Facebook account, and 25% for the Google account, stated that they changed their passwords because they realized that the old password was very weak and could compromise their other passwords and accounts.

3.3 Password Memorability and Write-down

Part of our lectures and recommendations consisted of educating the participants about how important it is for them not to write their passwords down on any item (notebook, on a desk, keyboard, monitor, wall, in their mobile phones etc.). Once a password is written down, it is no longer something to be cracked or guessed, but something to be located. A password, which is written down, can be easily found by search through user's personal stuff, like notebook, desk, diary, or user's manual [Zviran and Haga 1999]. But in an environment where users are managing multiple passwords for multiple different accounts, they start to use different strategies for coping with the password use and remembrance (usually they write their passwords down or share them with their friends or co-workers) [Grawe-

Table VII. Password Memorability

Answer	Phase	desktop comp.	notebook comp.	mobile phone	tablet device	University account	Facebook account	Twitter account	Google account
Yes	First	2 (6.06%)	4 (12.12%)	3 (9.09%)	2 (6.06%)	7 (21.21%)	6 (18.18%)	3 (9.09%)	7 (21.21%)
	Second	3 (12.50%)	2 (8.33%)	1 (4.17%)	(4.17%)	4 (16.67%)	3 (12.50%)	1 (4.17%)	4 (16.67%)
No	First	14 (42.42%)	25 (75.76%)	20 (60.61%)	3 (9.09%)	23 (69.70%)	24 (72.73%)	9 (27.27%)	20 (60.61%)
	Second	11 (45.83%)	20 (83.33%)	14 (58.33%)	1 (4.17%)	18 (75%)	19 (79.17%)	7 (29.17%)	15 (62.50%)

meyer and Johnson 2011]. In both phases of the study, we asked our participants questions related to password memorability and password write down: “Very often, computer users find it convenient to write down their password for one of these unfortunate times when they forget it. Did you do this too for your password?” and “Have you ever had difficulty remembering your password?”. The answers to both questions are summarised in Table VI and Table VII, respectively. In both tables, the first column represents the answers to the question (Yes, No), the second column represents the phase of the study (First, Second). The rest of the columns represent the percentage of users that chose the specific answer for the specific account. The results in Table VI show that users rarely write their passwords down. Even 18.18% of the users reported that they wrote down their password for their University account, and less than 10% for the rest of the accounts. From the results in Table VII we can realise that 21.21% of the users have problems with remembering their University account, 18.18% for the Facebook account, and 21.21% for the Google account. Seems like the passwords for the University, Facebook, and Google account are the most hard ones to remember. One possible explanation for this may lay in some of our previous findings where we discovered that majority of users’ passwords for these accounts were more complex in their structure than the passwords for the rest of the accounts. These results look promising, compared to the results reported by the authors Zviran and Haga [1999] who found that even 35.5% of the participants in their study wrote down their passwords.

4. CONCLUSION

The study investigates the effect of password security training on user’s practices regarding password creation, password use and management. We performed a pilot study on university students to explore their password characteristics and habits regarding password creating, using, managing and security. We collected our data by means of an online questionnaire. The survey consisted of two phases. Between the two phases, the students received lectures about the importance of creating strong and secure passwords, how to choose such passwords and how to manage them.

The results show that the passwords for the desktop and notebook account in the first phase most commonly consisted of lowercase letters only (15.15% for the desktop and 21.21% for the notebook account), regardless the fact that most of the users rated their data on their desktop and notebook computer as very important. We observe an improvement in the characteristics of the passwords for the desktop and notebook accounts in the second phase of the study: passwords for these accounts were mostly alphanumeric with mixed case letters and numbers (20.83% for the desktop and 29.17% for the notebook account). The results from the first phase show that many users never change their passwords since their first use, or change them less than once a year. The results of the second phase of the study look promising, since even 25% of the users, for the desktop computer, 33.33% for the notebook computer, 20.83% for the University account, 29.17% for the Facebook account, and 25% for the Google account, stated that they changed their passwords because they realized that the old pass-

word was very weak and could compromise their other passwords and accounts. 18.18% of the users reported that they wrote down their password for their University account, and less than 10% for the rest of the accounts. Users stated that they usually have problems remembering their University account (21.21%), their Facebook account (18.18%), and their Google account (21.21%). The lectures and recommendations had a positive effect regarding users' password characteristics and password length, but not quite positive regarding password change. Despite our efforts to educate the users about the importance of frequent password change, a large percent of users did not change their passwords following the lectures. The overall conclusion of this preliminary study is that users still lack of security knowledge. Lax security behaviour regarding rare password change and password write-down, still exists (the results show some improvement though since the research made by Zviran and Haga [1999]).

Our plans for future work include research about possible differences in the quality of passwords between students from different faculties and different fields of study. Also the differences in quality of passwords between organizatoins with defined security policies and those without one. A flexible password policies tailored to mitigate the risks users actually face in a combination with password checkers can help users create strong and easy-to-remember passwords. This work will serve as a starting point for our further research in this area where we want to determine whether our university password policies are useful to the students, and whether the students can easily apply them or the policies cause them problems when creating and using passwords.

REFERENCES

Anne Adams, Martina Angela Sasse, and Peter Lunt. 1997. Making Passwords Secure and Usable. In *Proc. of HCI on People and Computers XII (HCI 97)*. Springer-Verlag, 1–19.

Matt Bishop and Daniel V Klein. 1995. Improving system security via proactive password checking. *Computers & Security* 14, 3 (1995), 233–249.

Rachna Dhamija and Adrian Perrig. 2000. Deja Vu: A User Study Using Images for Authentication. In *Proc. of the 9th Conference on USENIX Security Symposium - Volume 9*. USENIX Association, 4–4.

Serge Egelman, Andreas Sotirakopoulos, Ildar Muslukhov, Konstantin Beznosov, and Cormac Herley. 2013. Does My Password Go Up to Eleven?: The Impact of Password Meters on Password Selection. In *Proc. of the SIGCHI Conference on Human Factors in Computing Systems (CHI '13)*. ACM, 2379–2388.

Beate Grawemeyer and Hilary Johnson. 2011. Using and Managing Multiple Passwords: A Week to a View. *Interact. Comput.* 23, 3 (2011), 256–267.

Delbert Hart. 2008. Attitudes and Practices of Students Towards Password Security. *J. Comput. Sci. Coll.* 23, 5 (2008), 169–174.

A.M. Horcher and G P Tejay. 2009. Building a better password: The role of cognitive load in information security training. (2009).

Markus Jakobsson and Mayank Dhiman. 2013. The Benefits of Understanding Passwords. In *Mobile Authentication SE - 2*. Springer New York, 5–24.

Robert Morris and Ken Thompson. 1979. Password Security: A Case History. *Commun. ACM* 22, 11 (Nov. 1979), 594–597.

Gilbert Notoatmodjo and Clark Thomborson. 2009. Passwords and Perceptions. In *Proc. of the Seventh Australasian Conference on Information Security - Volume 98 (AISC '09)*. Australian Computer Society, Inc., Darlinghurst, Australia, Australia, 71–78.

P. Cisar and S. Maravic Cisar. 2007. Password a Form of Authentication. (2007).

M A Sasse, S Brostoff, and D Weirich. 2001. Transforming the Weakest Link a Human/Computer Interaction Approach to Usable and Effective Security. *BT Technology Journal* 19, 3 (2001), 122–131.

Viktor Taneski, Boštjan Brumen, and Marjan Heričko. 2014. Password security no change in 35 years?. In *Proc. of The 37th International ICT Convention MIPRO 2014*. IEEE, 1507–1512.

Moshe Zviran and William J Haga. 1990. Cognitive passwords: The key to easy access control. *Computers & Security* 9, 8 (1990), 723–736.

Moshe Zviran and William J Haga. 1999. Password Security: An Empirical Study. *J. Manage. Inf. Syst.* 15, 4 (1999), 161–185.

M. Zviran and W. Haga J. 1993. A Comparison of Password Techniques for Multilevel Authentication Mechanisms. 36, 3 (1993).