"The Four Most-Used Passwords Are Love, Sex, Secret, and God": Password Security and Training in Different User Groups

Birgy Lorenz[1], Kaido Kikkas[1,2], and Aare Klooster[1]

[1] Institute of Informatics, Tallinn University, Narva Road 25, 10120 Tallinn, Estonia
[2] Estonian Information Technology College, Raja St 4C, 12616 Tallinn, Estonia
{Birgy.Lorenz,Kaido.Kikkas,Aare.Klooster}@tlu.ee

Abstract. Picking good passwords is a cornerstone of computer security. Yet already since the early days (e.g. *The Stockings Were Hung by the Chimney with Care* from 1973; we have also borrowed our title from the 1995 movie *Hackers*), insecure passwords have been a major liability. Ordinary users want simple and fast solutions – they either choose a trivial (to remember and to guess) password, or pick a good one, write it down and stick the paper under the mouse pad, inside the pocket book or to the monitor. They are also prone to reflecting their personal preferences in their password choices, providing telling hints online and giving them out on just a simple social engineering attack. Kevin Mitnick has said that security is not a product that can be purchased off the shelf, but consists of policies, people, processes, and technology. This applies fully to password security as well. We studied several different groups (students, educators, ICT specialists etc – more than 300 people in total) and their password usage. The methods included password practices survey, password training sessions, discussions and also simulated social engineering attacks (the victims were informed immediately about their mistakes).

We suggest that password training should be adjusted for different focus groups. For example, we found that schoolchildren tend to grasp new concepts faster – often, a simple explanation is enough to improve the password remarkably. Thus, we would stress the people and process aspects of the Mitnick formula mentioned above.At the same time, many officials and specialists tend to react to password training with dismissal and scorn (our study suggests that 'you cannot guess my password' is an alarmingly common mindset). Examples like 'admin', 'Password', '123456' etc have occurred even at qualified security professionals, more so at educators. Yet, as Estonia is increasingly relying on the E-School system, these passwords are becoming a prime target. Therefore, for most adult users we suggest putting the emphasis on policy and technology aspects (strict, software-enforced lower limits of acceptable password length, character variability checks, but also clearly written rulesets etc).

Keywords: passwords, security awareness, training, privacy, user behavior.

1 Background

Finding good passwords has been an important issue since the early days of computing [11]. Two decades later, things were still the same [2] – passwords were

L. Marinos and I. Askoxylakis (Eds.): HAS/HCII 2013, LNCS 8030, pp. 276–283, 2013.

short and ways to produce good passwords were complicated. The well-meaning attempt to add security by forcing frequent password changes resulted in users starting to write them down [1]. Nowadays, after two more decades, most passwords tend to be hard to remember but easy to crack.

A major security risk results from user-generated passwords, as among common users, comfort prevails over security [5]. At present, best passwords are considered to be at least 15 characters long and containing at least two numbers and one special character, making them practically impossible to crack due to the processing power needed [4]. However, getting the users to comply has presented a challenge [6] and without actual understanding the effect would be negligible [7]. Some researchers also suggest that a way to add contextual security it is safer to avoid passwords in common, internationally used languages. Native words are easier to remember and, with some tweaks, can result in passwords resistant to dictionary-based attacks [10].

Another issue is the exponential growth of password-using environments, making it very difficult to generate unique yet user-friendly passwords for all of them – even if some algorithm is used, and its pattern is usually easily distinguishable [8]. Various frameworks involving password testing or user training has been suggested [9], another way would be to use biometrics [12] or independent one-time passwords [13]. In Estonian context, using the national ID card infrastructure can be considered a good approach.

Several studies (e.g. Brown, 2004) point out two central flaws of user-generated passwords – personal origins and password reuse [3]. Our current study confirms most features outlined by Brown.

2 Methods

Our study consisted of two main stages. Stage I consisted of a survey among different groups with 341 respondents in total: 44 high school students, 51 vocational school students, 78 university students, 26 teachers/trainers, 35 ICT specialists, and 107 other adults (the „average Joe" comparison group). The survey was carried out in May 2012 for some groups and in September and October 2012 for others.

The survey used the snowball method with the 'seed' for each group being students of Pelgulinna Gymnasium (the high school group), Tallinn School of Economics (vocational school) and Master students of various ICT-related programs at Tallinn University (university), teachers and instructors (teachers) and ICT staff (ICT instructors, educational technologists, network administrators; ICT professionals) from the same facilities. Respondents from these groups were then asked to forward the questionnaire to other would-be respondents. The comparison group of 'other adults' was compiled purely on random personal contacts who then distributed the survey further on.

The 28-point survey was divided into four sections – current password use, personal password policy, e-safety awareness and the respondent's background. Response types included Likert scale, multiple choice as well as open-ended questions.

The second stage involved Internet safety training and discussion of the Stage I results among different groups, including primary school students. Password training

events included discussion about common password models, testing current password strength, learning about safe password storage options and ICT safety suggestions based "simple safety rules" or 12 easy steps model provided at the Arvutikaitse.ee (SafeComputer) website – e.g. using antivirus and firewall, regular software updates and backups, account types and policies, selective downloading, password security, caution with unknown e-mail attachments or web links, using authentication based on the national ID card, and also some behavioral tips (e.g. asking for help when needed, avoiding using computers when tired etc).

3 Results

The results from the Stage I survey reveal that the overall situation in password security and related awareness has plenty of room for improvement. While the groups and their presumed knowledge about the issue was chosen to be remarkably different (e.g. high school students versus people working as ICT professionals; this was also a reason to include the large 'other adults' group to represent a supposedly average level), the differences were notably smaller than anticipated.

More than 50 per cent of the respondents claimed to use only 4 or less different passwords, with most groups having the percentage over 75 and even among the ICT professionals they accounted for a small majority (only 46% used more than 4). 50% of university students, 65% of teachers and 62% of the generic 'other adults' group claimed to use shorter passwords than 9 characters. There was a visible correlation between using longer passwords and different passwords in different places (likely reflecting the overall security awareness or lack thereof). Teachers and ICT professionals were notably different – while professionals used stronger and variable passwords (they were also the only group making wider use of special characters), teachers rather fell to the opposite side (e.g. 81% using just 2-4 passwords).

Most passwords still consisted of letters and numbers (although change of case is widely used) – the only notable exception in this was ICT professionals. Special characters were not used by 3 of every 4, and those who did use them, mostly confined themselves to a small subset (notably period, again favored by ICT professionals). Overall, the most used components for passwords are one's birth date or a date of special meaning, either one's or his/her close person's nickname, one's favorite animal and 1-4 random numbers – only the last one of which could be recommended as a good practice. Random numbers were most favored by ICT professionals and the youngest group of students – this suggests that the awareness may be slowly rising.

Another often-recurring feature is the password model of "Room1000" (starting with capital letter and ending with numbers or vice versa) – the model is used by a strong majority (70-80%) of all groups. For comparison, the so-called CamelCaps model (a multi-word sentence, every word capitalized) was used relatively less, ranging from one third to half of the respondents in different groups.

Password storage practices also varied but widespread neglect was visible here as well. While a strong majority of the respondents picked the option „only in my

memory", this was likely exaggerated and a more realistic picture was revealed by studying other options.

While storing passwords on paper seems to be declining, it is still done by about one third of respondents (inside a notebook, hidden e.g. under the keyboard, locked up somewhere etc). About half of the respondents uses an electronic means but tend to neglect safer options like encrypted 'password safe' software (used by just 0-4 people in each group), rather storing passwords in a generic file or in a web browser.

Solutions when losing one's password show the overall preference towards password reminder (2/3 to 3/4). An intriguing point is that those who should know best – teachers and ICT professionals – do not like to use password reminders and secret phrases, using more controversial techniques instead. A sizable share of teachers (10 out of 26) favors their notebook as password storage, while about half of the ICT staff would just 'hack' (try different passwords, attempt bypass etc).

Using secret questions to retrieve/change passwords reflects some of the same lack of imagination seen at the password choice. The most popular options for the question seems to be 'favorite animal' for younger people (around 40%) and 'something personal' (also about 40%), ICT professionals also use the 'my first (teacher, car)' rather often. Given that knowing the person would provide a lot of clues for the question (as the 'personal' question is often also limited to a couple of generic options by the service provider), the situation is worrisome.

Further into password safety, it seems to be a common practice to share passwords with one's life partner (among adults, 30-50%) or a family member (20-25%). Sharing is especially common among the 'other adults' group (the 'general public'). Students usually share their password also with friends and sometimes with ICT support staff.

The survey also contained some questions about general awareness of computer security. While different aspects varied, the differences between groups were not substantial. On the one hand, most laptops (around 60%) and wireless networks (around 70%) had passwords and the majority of home computers had antivirus and firewall installed and updated. On the other hand, most home desktops did not use passwords, were mostly used with administrative (and in most cases, one common) account and the operating system was not regularly updated. A troubling notion: while the situation looked a little better for ICT professionals, the difference was not substantial – e.g. 26% of them did not update the operating system regularly either.

Some more observations about the lack of security awareness include:

- the majority of home computers were very weakly protected, at the same time only 1/3 of the respondents said that the computer was not used by people outside the family;
- slightly more than a half of the respondents use a PIN/screen lock on their cell phones (among teachers, the percentage was even lower at 38%), at the same time a visible minority uses the same device to store their passwords;
- less than 10% would lock their account or log out before leaving the computer for a longer period.

When asked to describe a good password, the common consensus clearly preferred the length of '7-14' to 'over 15' – the latter was given preference by less than 10%. While the importance of having symbols in different cases was acknowledged (60-70%) as well as using a mix of letters and numbers (about 70-80%), using special characters and refraining from using dictionary words were given very low priority (10-30%; here, the ICT professionals stood out as a group). Given a choice between a short but complicated and a long but simple password the latter got a little more votes, but the percentage ratio was just around 45 to 55.

The password training and discussion sessions at the Stage II of the study focused on finding out different attitudes and solutions for using passwords in a networked environment. We found that although there have been discussions about the need for media literacy training already at the kindergarten [14] privacy awareness is very low among younger students. Although the sites used for 'my first password' are mostly recreative and thus often considered 'unimportant' from the adults' point of view, this is where later password habits are rooted at.

Different user groups need different approaches. For example, working with different student grades showed that:

- grades 1-2 typically visit children's gaming sites and use simple 4-6 character passwords. They are however quick learners and develop healthy password habits when taught properly;
- grades 3-4 are typically already more involved on the Net – even on gaming sites, they understand the need to protect their virtual assets well and have often also had their first negative experiences with strangers online. Yet these students still trust adults and tend to reveal their passwords to them when asked (especially by teachers or ICT professionals). They also wrote passwords down to their notebooks (which then occasionally got lost or stolen). At the same time, they were probably the most receptive audience and quick adopters of better security practices;
- while Grades 5-6 were mostly similar in attitudes with their younger peers, notable change occurs at Grade 7, after which the attitudes fell more in line with high school students (more diversity, less trust in authority, more confidence in one's own knowledge);
- among the high school students and all adults, there was clear correlation between interest in security issues and the person's overall ICT skills. At the same time, we noted an unpleasant tendency of overconfidence in one's skills, especially among ICT professionals, teachers and Master students. In many cases, they were reluctant to believe that they need to improve. For example, some considered using password tools like storage software 'weak', instead proposing that they will remember all password (which, according to Stage I findings, is not always true). Some were genuinely amazed when some recurring patterns in password creation were shown to them.

In conclusion we see that it is important to understand background and behavioral patterns, learning ability before conducting any awareness training in this matter.

4 Discussion

Today's average Internet user faces a lot of passwords in his/her online life – several e-mail accounts, social networks, various e-services and workplace solutions would all need different passwords. In reality, people are lax and use at most four passwords that get rotated in different environments. Only a few consider the possibility of break-in as they think their password is 'good enough'. Passwords may be elaborate but they tend to be short – perhaps hard to guess but easy to crack by today's technical means. And if they are forced to be longer, the users start relying on easy-to-remember combos stemming from their personal life. Using special characters is rare – even if adding just one greatly improves the password's quality. Most importantly, if admins start to enforce stricter password policies without a thorough explanation and user training, this has almost no effect – at best, users will use their former short password mechanically doubled or tripled.

Most users at least attempt to memorize their passwords, but in our study, a lot of people used notebooks or similar places, the rest made heavy use of password reminders with generic secret questions (maiden name, favorite teacher or country etc) whose answers are rather easy to find online. Therefore, training users specifically on password storage security becomes essential.

The main aim of our study was to understand how people with different age and background create and store their passwords. We saw a lot of similarities, but the follow-up training sessions also revealed different issues and stances in different groups. For example, small children do not grasp the idea of secrecy – the understanding of proper password use tends to grow by time as some passwords get forgotten and some accounts broken in. At the same time, the youngest users were also the easiest to train – the change in password models resulting from the training was radical. Adults, especially with ICT background, often were the most reluctant trainees who needed 'proof' of their incompetence (anecdotal evidence also includes a meeting of ICT professionals during which everyone's password was cracked and presented to the owner afterwards).

Another common problem is password sharing with friends and partners. On the one hand, it is understandable that besides common home, children and finances, online resources are also shared. Yet actual cases suggest that following break-up, it is much easier to change a door lock or block a bank account than even remember all the online accounts that were used together; the situation grows worse if the ex-partner also knows the password models of the other side.

Studying the result of the current and also earlier surveys, one has to wonder why this issue has only but little approached from the angle of social engineering. There are no simple solutions for managing human behavior, and 'the problem between the keyboard and the chair' remains - but people can be trained and informed. While technical aids (tokens, ID card) can be beneficial, they are effective only where they are ubiquitous (e.g. education or public sector). With the border between work and home dissolving (e.g. BYOD or Bring Your Own Device), extra stress is put on corporate security as well (a part of which is that users create 'comfortable' passwords also at

their workplace) – the Mitnick formula of policies, people, processes and technology remains of prime importance.

5 Conclusion

While the topic is as old as first secrets hidden behind closed doors, the only valid solutions are still policies and training. We tend to have policies, but as long as users do not understand them thoroughly, passwords will stay easy to deduce and/or easy to intercept. Training works, but has to overcome many misconceptions – awareness training must be down-to-earth, sometimes also using 'shock therapy' by demonstrating the vulnerability in a direct manner (care must be taken not to violate any legal rights though).

Passwords that keep pace with today's technology should be at least 15 characters long and contain at least two numbers and one special character – in our study, 2% complied with the rule. Therefore constant and repeated reminders and awareness raising campaigns are needed.

Next steps in this area involve developing training units and exercises as well demo environment where people can test out their knowledge. It should not only be done thru survey testing, but also include real life situations, games and videos.

Acknowledgements. This research was supported by European Social Fund's Doctoral Studies and Internationalisation Programme DoRa, which is carried out by Foundation Archimedes and also by Estonian Information Technology Foundation.

References

1. Adams, A., Sasse, M.A., Lunt, P.: Making passwords secure and usable. People and Computers, 1–20 (1997)
2. Belgers, W.: UNIX password security (1993) (retrieved July 1, 2009)
3. Brown, A.S., Bracken, E., Zoccoli, S., Douglas, K.: Generating and remembering passwords. Applied Cognitive Psychology 18(6), 641–651 (2004)
4. Burnett, M.: Ten Windows Password Myths. Online Document (2002), http://www.securityfocus.com/infocus/1554
5. Cazier, J., Medlin, D.: Password Security: An Empirical Investigation into E-Commerce Passwords and Their Crack Times. Information Systems Security (1065-898X) 15(6), 45 (2006)
6. Charoen, D., Raman, M., Olfman, L.: Improving End User Behaviour in Password Utilization: An Action Research Initiative. Systemic Practice and Action Research 21(1), 55–72 (2008)
7. Chaumont, S.: Security Awareness Training: Passwords. Illinois banker (0019-185X) 97(11), 13 (2012)
8. King, D.: Unforgettable Passwords. American libraries (Chicago, Ill.) (0002-9769) 43(11/12), 57 (2012)

9. Kulkarni, D.: A Novel Web-based Approach for Balancing Usability and Security Requirements of Text Passwords. International Journal of Network Security & its Applications (0975-2307) 2(3), 1 (2010)
10. Malempati, S., Mogalla, S.: Enhanced Authentication Schemes for Intrusion Prevention using Native Language Passwords. International Journal of Computer Science Issues (IJCSI) (1694-0784) 8(4), 356 (2011)
11. Metcalfe, B.: The Stockings Were Hung by the Chimney with Care. RFC 602 (1973), http://tools.ietf.org/html/rfc602
12. O'Gorman, L.: Comparing passwords, tokens, and biometrics for user authentication. Proceedings of the IEEE 91(12), 2021–2040 (2003)
13. Rubin, A.D.: Independent one-time passwords. Computing Systems 9(1), 15–27 (1996)
14. Vinter, K., Siibak, A., Kruuse, K.: Meedia mõjud ja meediakasvatus eelkoolieas. Haridus 4, 11 (2010)