Essential Lessons Still Not Learned? Examining the Password Practices of End-Users and Service Providers

Steven Furnell[1,3] and Nina Bär[2]

[1] Centre for Security Communications and Network Research, Plymouth University, Plymouth, United Kingdom
[2] Chemnitz University of Technology, Chemnitz, Germany
[3] Security Research Institute, Edith Cowan University, Perth, Western Australia
sfurnell@plymouth.ac.uk, nina.baer@psychologie.tu-chemnitz.de

Abstract. Password authentication remains the dominant form of user authentication for online systems. As such, from a user perspective, it is an approach that they are very much expected to understand and use. However, a survey of 246 users revealed that about one third chose weak passwords, including personal information or dictionary words. To prevent such forms of bad security behavior, service providers should offer support, but the reality of the situation suggests that tangible weaknesses can exist amongst both parties, and thus despite their long-recognised importance, good password practices have yet to become an established part of our security culture. An experimental study was conducted in order to investigate the effect of providing password guidance upon end users' password choices. The findings revealed that the mere presentation of guidance (without any accompanying enforcement of good practice) had a significant effect upon the resulting password quality.

Keywords: Password guidance, authentication, end user, security behavior.

1 Introduction

Passwords continue to be the most common context in which people come into contact with security, representing the de facto authentication method on desktop and laptop computers, as well as the standard mode for requesting authentication on the various websites and other online services that now require it. However, in spite of their long-established and widespread use, the underlying password choices made by end-users continue to exhibit a variety of weaknesses. Put simply, good password selection is not a skill that many users seem to possess by nature, and so they require appropriate awareness and support in order to do things properly. Unfortunately, the extent to which this is provided for them is often insufficient, thus leaving them to perpetuate a problem across multiple systems and accounts.

This paper examines the situation based upon the current practices of end-users and service providers, revealing notable gaps in both cases. It then continues to investigate the improvements in password practices that can result from relatively minor

L. Marinos and I. Askoxylakis (Eds.): HAS/HCII 2013, LNCS 8030, pp. 217–225, 2013.

additional efforts on the provider side, by simply ensuring that relevant guidance is presented to users to inform their password choices.

2 A Survey of End-User Practices

In order to assess the degree to which good practices are now embedded within password usage, a series of related questions were incorporated in to a wider survey of end-user security practices (with the full question set also spanning issues such as use of antivirus and Internet security tools, and security of mobile devices).

The overall results are based on a respondent group of 246, of which 108 are classified as 'general public' and 138 were 'IT students'. The public sample was captured during a science and technology showcase event, at which online security was highlighted as one of the key issues. Meanwhile, the 'IT students' were newly commencing the first year study for an undergraduate degree in computing, and were approached to complete the questionnaire during their first week of study, before receiving any specific tuition in relation to security topics. Thus, as a respondent group, they can be considered to have declared an explicit interest in IT (and may therefore be more regular and active users of it), but they should not be assumed to inherently be any more aware in relation to security issues than the wider population. The first notable finding in relation to passwords was that users can potentially have a fair number of them to manage. Respondents were asked how many systems or sites they used that required a password, and the overall results are depicted in Figure 1. Looking within the sub-population, the IT students were (perhaps unsurprisingly) facing more of a password management challenge, with only 8% of them responding in the '1-5' category and 39% reporting to use 16+ password-based systems.

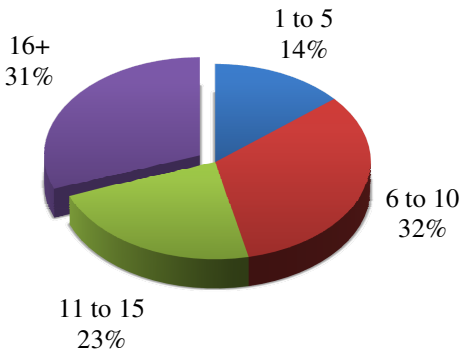

Fig. 1. Number of systems or websites requiring passwords

Of course the number of systems or sites used does not necessarily map onto an equivalent number of distinct passwords, and so the respondents were also asked to broadly indicate their practices in this regard. The majority (54%) indicated that they have a set of passwords that they choose from, while 27% claimed to have a different

on for each site, and 17% suggested that they used the same one on every system (the remaining percentage left the question unanswered).

Having established a clear dependency upon password-based approaches, the final segment of password-related questions helped to further demonstrate the extent to which users' practices can be often be less than ideal. Respondents were presented with a series of potential statements about the password used on their most valuable system, and asked to indicate all that applied. The average responses across the whole group are presented in Table 1, and it can be seen that good practice tends to vary.

Table 1. Responses to statements around password usage

Statement	Agreement (n=246)
It is at least 8 characters long	82%
It has alphabetic and numeric characters	84%
It includes other characters (e.g. punctuation symbols)	49%
It uses a word you would find in a dictionary	18%
It is based on personal information about me	26%
I have changed it since I started using it	36%
I change it regularly	21%
I have shared it with other people	6%
I have forgotten it and had to reset/recover it	10%

From these overall findings, the only one that stands out as suggesting the good practice is properly embedded is the fact that only 6% report to have shared their password. This suggests that the vast majority of users understand and accept the premise of the password as being their authentication secret. Beyond this, however, there are tangible proportions of weaker practice in all of the areas considered. While there was no significant difference between the populations in terms of baseline length, there was a tangible difference in how they were reportedly composed. For example, 91% of IT students reported using passwords containing both alphabetic and numeric characters, as opposed to only 76% of the general public group. Even more notably, when asked about the use of punctuation characters, these were incorporated by 59% of the students versus only 36% of the public.

Findings suggest that IT students are marginally better in terms of good practices such as changing their passwords regularly, not sharing, and not having forgotten their details. This sub-group was also significantly better in terms of not using personal information (78% versus 68%), but this still leaves tangible proportions in both cases (and some 26% of the respondent group overall) that were admittedly using passwords based upon personal details. Moreover, largely equal proportions from both groups (averaging 18% of the respondents overall) reported using dictionary words. Thus, assuming that the categories of personal information and dictionary words do not intersect too greatly, this easily represents more than a third of respondents making password choices that would contravene standard guidance, before one even gets to the stage of looking at password composition.

3 Assessing Service Provision

Given that some users clearly exhibit inclinations towards making weaker choices, it is relevant to consider the extent to which they may be supported and guided towards doing things properly. An indication of this can be gained by looking at the password guidance and enforcement offered by leading websites. A prior study from Furnell considered ten leading sites, and discovered that half provided little or no guidance on password selection when users initially registered and set up their accounts [1]. Of the sites that did provide guidance, only two went to the extent of providing links to comprehensive guidance pages covering tips for password selection, use and protection. By contrast, some sites provided no password guidance at all at the point of registration, and most fell somewhere between the extremes, providing some indication of criteria for selecting passwords, but no wider suggestions for protecting them once chosen.

In addition to the variability of guidance, the sites also varied significantly in the degree to which they enforced good password practices. As the summary presented in Table 2 illustrates, the level of support is by no means uniform and (in many cases) is below that which one might consider desirable [1].

Table 2. The varying enforcement of password restrictions on websites

Site	Enforce min length (+max if approp)	Prevents Surname	Prevents User ID	Prevents 'password'	Prevents dictionary words	Enforces composition	Prevents reuse
Amazon	6	×	×	×	×	×	×
eBay	6-20	×	✓	✓	×	✓	✓
Facebook	6	✓	×	✓	~ (1)	×	×
Google	8	×	✓	✓	✓	×	✓
LinkedIn	6	×	×	✓	×	×	×
Twitter	6	×	×	✓	✓	×	×
Wikipedia	×	×	✓	×	×	×	×
Windows Live	6-16	✓	✓	✓	×	✓	×
WordPress	4	×	✓	✓	×	×	×
Yahoo!	6-32	✓	✓	✓	×	×	×

(1) Provision is only made when the user changes their password.

In view of these findings, it seems fair to suggest that users cannot rely upon the sites they are using to be proactive in safeguarding their interests. At the same time, without the provision of associated guidance, it is difficult for users themselves to ensure that they are using passwords as safely as possible.

4 Assessing Password Selection in Practice

Having critiqued the websites, it was hypothesized that the provision of credible guidance would help to ensure that users made better password choices. In order to test this in practice, an experimental study was mounted that required users to choose passwords as part of a wider set of activities.

Choosing a secure password as a form of security behavior is influenced by a set of factors perceived by the user. Huang et al. [2] suggest a model including knowledge, controllability, awareness, severity and possibility as determinants of a users' intention to follow security practices. The more end users know about the rationale of threats like password cracking and the better their understanding of such threats is, the more likely they will adopt a good security practice. The participants who stated in the survey that their password includes personal information or dictionary words might just not know that passwords can be cracked by dictionary attacks. By implementing password guidance on websites providers can help to explain that issue. When users are shown how to prevent or predict threats they feel much more comfortable and in control of the situation. The use of immediate feedback on their password choice, such as the use of a password strength meter, can enhance awareness that a proposed choice is too weak and help to ensure that even people without knowledge about the topic feel in control to protect their data. However, the compulsion to follow good password practices is nevertheless related to the perceived severity of consequences in case the password might be cracked. End users often indicate that even if their passwords were cracked they would not be concerned because they would not attach much importance to the consequences. That might be the case for passwords on accounts/systems of less personal relevance, but when asked for their most valuable account users should indeed be aware of the severity of negative consequences, especially as people are typically concerned about the privacy of the data they provide to websites. In contradiction to this, however, that concern is often not noticeable in their online actions [3]; mostly because of the immediate benefit of more convenience. Taking into account that users are willing to trade-off concerns about their online security for convenience, it seems likely that the additional influence of the subjective possibility of being a victim of online attacks is by far underestimated. ''I know my password is not strong, but I don't think anyone will have any interest in cracking my password and breaking into my computer'' is what participants answered when asked for their opinion about password security [4].

4.1 Experimental Design

To investigate the effect of providing security guidance upon the actual quality of passwords two versions of a website were tested in a between-design. Unbeknownst the participants, there were two versions of the site (one that paid attention to usability good practice, and the other which did not – see Figure 2), and they were not aware

that they were being assigned to a particular version. The initial task for the users was to register on the site by selecting a username and password. The experimental group was shown one version of the website which paid attention to good security usability including password guidance. They were provided with guidelines how to create a secure password and a password strength meter as immediate feedback on their password choice. The control group was shown a second version of the same website which did not contain any guidance or feedback on passwords.

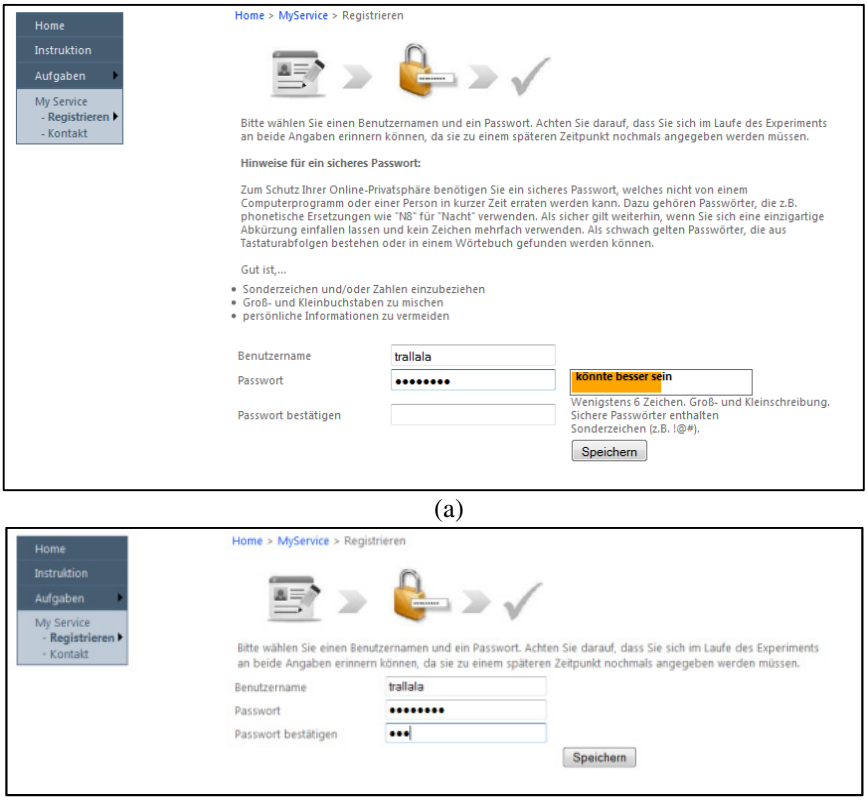

Fig. 2. The two variants of the website – (a) with and (b) without password guidance

For the experimental group the password guidance advised them in the following way: "For protecting your online privacy you need a safe password, i.e. one which cannot be easily guessed by a computer program or an individual in a short period of time. This includes passwords with phonetic replacements, e.g. 2nite for tonight. Furthermore, it is advised to create a unique acronym and not to repeat characters. Weak

passwords consist of keyboard patterns or can be found in a dictionary. It is good…(1) to include punctuation marks and/or numbers, (2) to mix capital and lowercase letters and (3) to avoid using personal information." Both groups were instructed to create a username and a password which both could be memorized throughout the whole experiment. Neither variant of the website enforced password selection rules, and on the version that included password guidelines there was still no obligation for the participants to read them. As such, any differences in the resulting password behavior would be attributable to the mere provision of guidelines.

4.2 Procedure

The participants were being asked to use a website and assess aspects of its usability. They were not made specifically aware that attention would be given to their password choices, and they were simply advised that they were participating in a website usability study (i.e. from the user perspective, choosing a password was just something they needed to do in order to get started, rather than being a central focus of the task). The users were, however, instructed to select a new password rather than one that they already used elsewhere. The basis for this was to both enable the study to assess their password selection practices, and to reduce the risk of them inadvertently divulging a password that they already used when it came to the later analysis. Having successfully registered, the users were then required to use the password to log in and comment upon the website's usability (the results of which form part of a wider HCI study, which is out of scope for this paper).

4.3 Sample

A total of N=27 participants (17 female, 10 male) were involved in the initial study. The mean age was M = 27.3 years. The experimental group (N=13) and the control group (N=14) did not differ in terms of the time they spent online for private purposes or other control variables such as affinity for technology.

4.4 Results

The resulting password choices were rated using a subset of the prior criteria from Table 1 that could be measured at the point of password creation. Specifically, a point could be scored for a password satisfying each of the following (thus giving a maximum of 5 points for good choice):

- at least 8 characters long
- composed of both alphabetic and numeric characters
- using other characters (such as punctuation symbols)
- not based upon a dictionary word
- not based upon personal information

Table 3. Summary results from study participants

	Used at least 8 characters	Used alphanumeric characters	Used other characters	Used non-dictionary	Avoided personal info
Guided (n=13)	85%	85%	62%	54%	92%
Unguided (n=14)	50%	64%	7%	50%	64%

It is arguable that the 8-character minimum is not a particularly secure baseline, but it was nonetheless the best of the set assessed from the earlier group in Table 2 and so forms a foundation on that basis. The results revealed a significant difference between those receiving guidance and those attempting to select passwords without it ($t(25)=3.82$, $p=.001$, $d= 1.5$). The mean for the former group was $M=3.8$ out of 5, whereas the unguided users averaged just $M=1.9$. The qualitative analysis of the individual cases revealed that those without guidance were notably more inclined to use personal information in their passwords, and far less likely to have considered the use of character types beyond alphanumeric. Table 3 summarises the overall performance of the two groups against each of the assessment criteria.

Although the results are only based upon a small sample, they nonetheless appear to offer a clear message in terms of the effectiveness of providing password guidance versus leaving users to their own devices. Although it can be argued that the users may not have been choosing typical passwords because they knew it was only being used in a study, the fact remains that all users were operating in this context and those receiving guidance nonetheless chose better. So, it is notable that the guidance even made a difference in this context (i.e. with a site they would be unlikely to value).

5 Conclusions

The paper has clearly evidenced that, that despite our long-standing use and familiarity with them, some significant problems surrounding passwords have yet to be resolved. Although the sample population in the practical study is currently small, the overall message emerging from the collective findings in the paper remains clear: users readily admit to making weak password choices, websites do not guide on or enforce good practice as well as they could, and yet the experiment clearly suggests that even the basic provision of guidance can help to deliver a tangible improvement. As such, there appear to be clear lessons to be learnt that could help to uplift authentication practices while passwords continue to be retained as a primary method.

Building upon these findings, it is intended that the research to benchmark the effect of providing password guidance will continue with a larger and more diverse

sample of users. If the later findings continue to support the same conclusions, then we believe this should represent a persuasive message regarding appropriate baseline standards that websites (and organisations) ought to be following in supporting their users' security practices.

References

1. Furnell, S.M.: Assessing password guidance and enforcement on leading websites. Computer Fraud & Security, 10–18 (December 2011)
2. Huang, D.-L., Rau, P.-L., Salvendy, G.: Perception of information security. Behaviour & Information Technology 29(3), 221–232 (2010), doi:10.1080/01449290701679361
3. Davinson, N., Sillence, E.: It won't happen to me: Promoting secure behaviour among internet users. Computers in Human Behavior 26(6), 1739–1747 (2010), doi:10.1016/j.chb.2010.06.023
4. Huang, D.-L., Rau, P.-L., Salvendy, G., Gao, F., Zhou, J.: Factors affecting perception of information security and their impacts on IT adoption and security practices. International Journal of Human-Computer Studies 69(12), 870–883 (2011), doi:10.1016/j.ijhcs.2011.07.007