Password Generation and Search Space Reduction

Kirsi Helkala and Einar Snekkenes
Norwegian Information Security Laboratory, NISlab,
Gjøvik University College, Norway,
Email: {firstname.surname}@hig.no

***Abstract*— It is easy for humans to design passwords that are easily remembered. However, such passwords may have a predictable structure, making exhaustive search feasible. We have divided human-generated passwords into three categories: Non-word passwords, Mixture passwords, and Word passwords; depending on their overall structure. Within these categories, we have analyzed the search-space reduction of several common password sub-structures. From this analysis, we have derived guidelines that yield strong passwords within in each password category. Our results contribute towards the goal of achieving both strong *and* memorable passwords.**

***Index Terms*— Password security, password policy, search space reduction, personnel authentication**

I. Introduction

Passwords are only as strong as the password-designing process. Random passwords can only be produced by random password generators. However, the generated strings might be difficult to remember, especially if someone has many accounts and therefore many different passwords. Humans can easily create memorable passwords, but this also creates the problem that their generation process is guessable, e.g. following structures of certain language [1] or themes [2]. Therefore, human-made passwords are less secure than random passwords.

To help users to generate good passwords, there are guidelines for password creation. However, such guidelines are very general, like those listed in [3], and may not be helpful for all users, given the variety of memorizing techniques. In order to overcome this problem, experts generally recommend [4] a system for evaluating each password against some metric and rejecting the weak ones, rather than mandating a certain number of characters from some character set.

The given guidelines are often based on the use of common knowledge, and not based on scientific computations. Statements such as "Use at least 2 digits, 2 lower case letters, 2 upper case letters, and 2 special characters" might misleadingly guide users into designing passwords with exactly the same number of characters and in the same order as the above statement, such as *12asLK!?*. Such passwords are weaker than the guidance intends, because it reveals a pattern to an adversary. The original meaning was to encourage users to design passwords longer than 8 characters and with characters from all available sets. If the characters were taken randomly from each set, the password would have been quite strong.

In our work, we have computed how much information the adversary gains when the password policy and the generation process are revealed. Based on the findings in [5], [6], we divided human-generated passwords into three categories: Non-word passwords, Mixture passwords, and Word passwords. Non-word passwords are character strings, which do not contain any real words that are found in the dictionary, names, locations etc. However, they can contain letters. Mixture passwords are character strings containing both word and non-word part(s), e.g. *T!today65?* has two non-word parts around the word part in the middle. Word passwords are then strings, which are either pure dictionary words, e.g. *password* or modifications of them e.g. *P@$$W0RD*.

The findings of the information leakage are further used to provide password-generation guidelines for each password category, in such as way that, even if the adversary knows the guidelines, the passwords generated according to these guidelines can be considered as secure.

The remainder of the paper is structured as follows. The analysis is presented in Section II. Section III provides the guidelines for password design. The comparison and discussion of our results and the results of related work is in Section IV. Section V concludes the paper.

II. Analysis of Password Structure

The analyzed cases are shown in Fig. 1. The minimal information which the adversary would gain is the general password policy. In this paper, the basic policy is "Minimum length of 8 characters, maximum length of 14 characters and all visible keyboard keys (except space) are allowed." With a Norwegian keyboard, the number of characters is then 105 and therefore, the maximum password entropy is 94.01 bits, computed as follows

$$\log_2 \sum_{i=8}^{14} 105^i = 94,01 \text{ bits}. \quad (1)$$

This baseline is used when the revealed information is computed with the following formula

$$\mathrm{H}_{Case} = 94,01 - \log_2 \mathrm{C}_{\mathrm{Case}}. \quad (2)$$

Manuscript received October 14, 2008; revised January 19, 2009; accepted January 31, 2009. The work has received financial support from the Research Council of Norway under grant 158777/530.

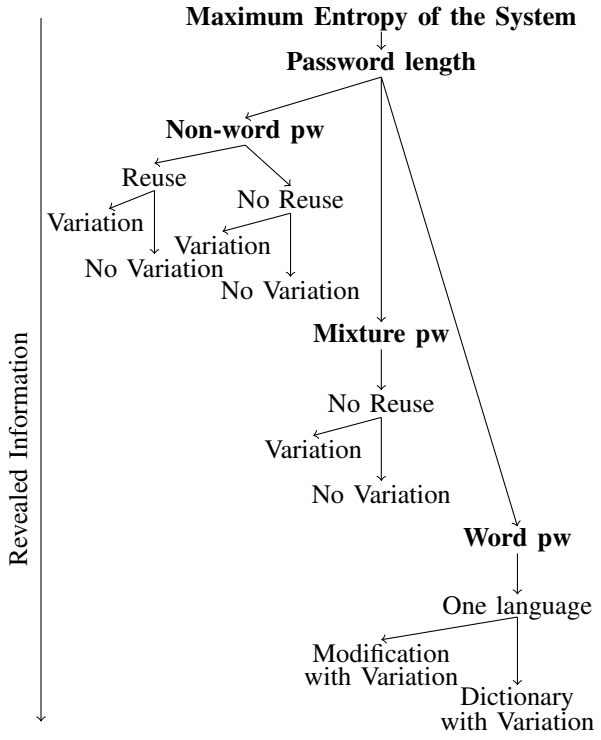

Figure 1. The analysis cases of our study.

We call a password *a good password*, when, given information about the password structure, the revealed information in bits is less than half of the baseline bits, i.e. less than 47 bits.

In the next case, in addition to general policy, the adversary knows the length of the password. The rest of the analysis is divided into three cases: A Non-word, a Mixture and a Word password. A Non-word password does not contain any Norwegian words, a Mixture password contains both Norwegian words or a word and extra characters, and Word passwords contain only words. We use four character sets (digits $|\mathrm{D}| = 10$ (cardinality), lower case $|\mathrm{LC}| = 29$ and upper case letters $|\mathrm{UC}| = 29$, and special characters $|\mathrm{SC}| = 37$). Because we do not have statistics of the most commonly used password characters, we assume a uniform distribution, when selecting characters from each of the above character sets.

A. Knowing the Password Length

In this case, the adversary knows only the system guidelines and length of a password. When only the length l, in addition to the number of the allowed characters cs, is known, the size of the effective search space is

$$\mathrm{C}_{Length} = cs^{l}. \tag{3}$$

The use of Formula 3 gives us following results: With an 8-characters password, the adversary knows 40.3 bits and with a 14 characters long password, the adversary knows 0.01 bits. If the adversary learns that a password was actually 7 characters long, he would have learned 47 bits. This suggests that passwords shorter than 8 characters are *not good*.

B. Human Design Passwords

Password strength depends on the password-design process. Maximum password strength is achieved when each password character is drawn independently and a uniform distribution is used. Usually, this is not the case when people design their own passwords.

Human-designed passwords can be Non-word, Mixture or Word passwords. Non-word password do not contain sub-strings that can be found in a dictionary e.g *NT*-Ke0*, Mixture passwords contain some words and extra characters e.g *4seasons1year* and Word passwords contain only words e.g *SkiingIsTheBestIKnow*. We show which design processes within each category provide good passwords and which do not. The analysis shows that the main criterion for designing good passwords is to vary the characters used and the placements of characters within each password-design session.

Non-word passwords. The analysis is divided into four sub cases.

- NW**rapu**: **r**eused characters are **a**llowed and the **p**attern of character placement in a password is **u**nknown.
- NW**rapk**: **r**eused characters are **a**llowed and the **p**attern of character placement in a password is **k**nown.
- NW**rdpu**: **r**eused characters are **d**enied and the **p**attern of character placement in a password is **u**nknown.
- NW**rdpk**: **r**eused characters are **d**enied and the **p**attern of character placement in a password is **k**nown.

We assume that if a person always designs passwords with the same structure, the pattern of the password is known.

Computations. The size of the Non-word password search space is

$$\mathrm{C}_{\mathrm{NonWord}} = f_1 g_1 \times f_2 g_2 \times f_3 g_3 \times f_4 g_4 - \mathrm{W}, \tag{4}$$

where functions g_i, computed with (5)-(8), give the cardinality of each character set used in a password and functions f_j, computed with (9)-(12), give the number of all possible combinations of character placement for each set in a password of length l. W stand for the number of possible words within letter combinations. These combinations are subtracted from the total number of the combinations, because Non-word passwords do not contain words. In these formulae, uc stands for the number of upper case letters, lc for lower case letters, d for digits, and sc for special characters.

The cardinality functions g_i are as follows

$$g_1(uc) = \begin{cases} 29^{uc}, & \text{reuse allowed} \\ \frac{29!}{(29-uc)!}, & \text{reuse denied} \end{cases} \tag{5}$$

$$g_2(lc) = \begin{cases} 29^{lc}, & \text{reuse allowed} \\ \frac{29!}{(29-lc)!}, & \text{reuse denied} \end{cases} \tag{6}$$

$$g_3(d) = \begin{cases} 10^d, & \text{reuse allowed} \\ \frac{10!}{(10-d)!}, & \text{reuse denied} \end{cases} \quad (7)$$

$$g_4(sc) = \begin{cases} 37^{sc}, & \text{reuse allowed} \\ \frac{37!}{(37-sc)!}, & \text{reuse denied} \end{cases} \quad (8)$$

Equations (9)-(12) are character-placement combination functions. These functions will get a value 1 if the pattern of the password is known. In other words, the adversary knows which characters in a password are digits, upper case letters, etc. When the pattern is unknown, the placement combinations are computed as follows

$$f_1(l, uc) = \binom{l}{uc} \quad (9)$$

$$f_2(l, uc, lc) = \binom{l-uc}{lc} \quad (10)$$

$$f_3(l, uc, lc, d) = \binom{l-uc-lc}{d} \quad (11)$$

$$f_4(l, uc, lc, d, sc) = \binom{l-uc-lc-d}{sc} \quad (12)$$

The number of passwords containing single or multiple words with a length of $(uc + lc)$ letters written both forwards and in reverse transformation, W, is computed with (13). We have simplified the subtraction, considering only the passwords containing words formed from all the letters in a particular password. The number of words, aw, shown in Table III, were provided by the Norwegian Text Laboratory.

$$W = [l - (uc + lc) + 1] \times 2aw \times f_3 \times g_3 \times f_4 \times g_4. \quad (13)$$

Example. As an example of the use of formulae, we show a situation in which a 10- character password ($l = 10$) contains 1 digit ($d = 1$), 1 lower case letter ($lc = 1$), 4 upper case letters ($uc = 4$) and 4 special characters ($sc = 4$). The reuse of the characters is allowed and the pattern is unknown. The number of words with a length of 5 letters is taken from Table III. Because the reuse of characters is allowed, we obtain the following cardinalities for the sets

$$\begin{aligned} g_1(4) &= 29^4 \\ g_2(1) &= 29 \\ g_3(1) &= 10 \\ g_4(4) &= 37^4. \end{aligned} \quad (14)$$

The combinations of the character placements will then be

$$\begin{aligned} f_1(10, 4) &= \tbinom{10}{4} = 210 \\ f_2(10, 4, 1) &= \tbinom{10-4}{1} = 6 \\ f_3(10, 4, 1, 1) &= \tbinom{10-4-1}{1} = 5 \\ f_4(10, 4, 1, 1, 4) &= \tbinom{10-4-1-1}{1} = 1. \end{aligned} \quad (15)$$

These will then yield the search space size of

$$\begin{aligned} \mathrm{C} \quad &= 210 \times 29^4 \times 6 \times 29 \times 5 \times 10 \times 37^4 \\ &\quad -[10 - (4 + 1) + 1] \times 2 \times 20767 \times 5 \times 10 \times 37^4 \\ &= 2.42 \times 10^{18} \end{aligned} \quad (16)$$

which will reveal information of

$$\mathrm{H} = 94,01 - \log_2 2.42 \times 10^{18} = 32.9 \text{ bits}. \quad (17)$$

TABLE I.
REVEALED KNOWLEDGE OF NON-WORD PASSWORDS. THE USED SETS ARE DIGITS (D), UPPER CASE (UC) AND LOWER CASE LETTERS (LC), AND SPECIAL CHARACTERS (SC). THE NUMBERS IN EACH CHARACTER SET COLUMN GIVE THE NUMBER OF CHARACTERS USED FROM EACH SET IN THE PASSWORD-DESIGN PROCESS. GOOD PASSWORDS ARE IN BOLD.

Pw L	Nr D	Nr LC	Nr UC	Nr SC	NW-rapu Bits	NW-rapk Bits	NW-rdpu Bits	NW-rdpk Bits
10	10	0	0	0	60.8	60.8	72.2	72.2
	9	1	0	0	55.9	59.3	64.0	67.4
	8	1	1	0	51.2	57.7	57.0	63.5
	0	0	0	10	**41.9**	**41.9**	**43.8**	**43.8**
	0	0	1	9	**38.9**	**42.3**	**40.5**	**43.8**
	0	1	1	8	**36.1**	**42.6**	**37.3**	**43.8**
	0	0	5	5	**35.7**	**43.7**	**36.6**	**44.6**
	1	4	4	1	**34.0**	**46.6**	**34.6**	47.2
	1	1	4	4	**32.9**	**45.6**	**33.5**	**46.1**
	0	2	3	5	**32.4**	**43.7**	**33.0**	**44.3**
8	8	0	0	0	67.4	67.4	73.2	73.2
	6	1	0	1	58.2	64.0	60.9	66.7
	0	0	0	8	52.3	52.3	53.5	53.5
	1	1	0	6	48.8	54.6	49.4	55.2
	0	0	4	4	47.6	53.7	48.2	54.3
	1	1	1	5	**46.5**	54.9	**46.9**	55.3
	2	2	2	2	**46.2**	57.5	**46.5**	57.8
	0	1	3	4	**45.6**	53.7	**46.0**	54.1
	1	1	3	3	**45.5**	55.6	**45.8**	55.9
	0	3	3	2	**45.3**	54.4	**45.7**	54.8
	1	3	2	2	**45.3**	56.0	**45.5**	56.2
	0	2	3	3	**45.0**	54.1	**45.3**	54.4

Other examples of the information revealed in each of four cases with a password length of 8 and 10 are shown in Table I.

Results. In summary, passwords are *not good* if they consist only of digits, or of digits and letters only either from the lower case letter set or the upper case letter set. The best passwords contain some special characters and characters from other sets, so that the number of digits is as low as possible.

When concentrating only on strong passwords (the bold entropies in Table I, we find the following. Comparison of the "reuse of characters allowed" -columns (*NWrapu* and *NWrapk*) to "reuse of characters denied" -columns (*NWrdpu* and *NWrdpk*), shows that the revealed information is rather similar. When characters are from several sets and the most of them are not digits the difference between cases gets smaller, and so do the actual revealed information entropies.

The difference in bits is significant, when comparing "pattern-unknown" columns (*NWrapu* and *NWrdpu*) with "pattern-known" columns (*NWrapk* and *NWrdpk*). This finding strongly supports the need to change the character pattern in each password-design session. According to Table I, it is possible to design a *good* Non-word password of length of 8 characters.

Mixture passwords. Mixture passwords contain both a word and a non-word component. The following analysis is divided into two sub-cases with three different possibilities for the extra character set comprising either a set of

digits, special characters, or digit and special characters. Here, we consider only those cases where the reuse of characters is denied.

- M**pu**: the placement **p**attern of the word(s) and extra character(s) is **u**nknown.
- M**pk**: the placement **p**attern of the word(s) and extra character(s) is **k**nown.

In order to compute the worst case scenarios, we only consider dictionary words as words, not their modification. Their modification is discussed further in the section below on Word passwords.

Computations. The size of the Mixture password search space is

$$C_{Mixture} = c_{wo}c_{pe}(\prod_{p=1}^{w} aw_p(lw_p))\frac{\mathrm{es}!}{(\mathrm{es}-n)!}, \quad (18)$$

where $aw(lw)$ is the number of lw -length words, w the number of words, es the size of the extra character set and n the number of extra characters used in non-word parts of password. The combination of different word orders c_{wo} is computed with (19), where w_{sl} is number of same-length words. The combinations of extra character places between words c_{pe} was noted, so as to follow the numbers in Pascal's Triangle, which is then used to compute (20). Again, if the pattern is known, then (19) and (20) are 1. If the pattern is unknown, then the formulae are as follows

$$c_{wo} = \frac{w!}{w_{sl}!} \quad (19)$$

$$c_{pe} = \sum_{i=1}^{k} \binom{n-1}{i-1}\binom{w+1}{i}, \quad (20)$$

where $n \geq 1$ and $k = \min(n, (w+1))$.

Example. As an example of the use of the formulae, we show a case where a password contains 2 words ($w = 2$), both with a length of 3 letters ($w_{sl} = 2$), and 4 digits ($n = 4$, $es = 10$). The possible word order combinations are

$$c_{wo} = \frac{2!}{2!} = 1 \quad (21)$$

and the possible placement combinations among digits and words are

$$c_{pe} = \sum_{i=1}^{3} \binom{4-1}{i-1}\binom{2+1}{i} = 15. \quad (22)$$

These yields the following search space size

$$C = 15 \times (3048^2)\frac{10!}{(10-4)!} = 7.02 \times 10^{11}, \quad (23)$$

which leads to revealed information of

$$\mathrm{H} = 94,01 - \log_2(7.02 \times 10^{11}) = 54.7 \text{ bits}. \quad (24)$$

Some other examples of the revealed information of Mixture passwords with a length of 8 and 10 characters are shown in Table II.

Results. The revealed information entropies in Table II show that a *good* Mixture password cannot be shorter than 10 characters. Furthermore, even with 10 characters, only a small number of the passwords can really be considered as *good*.

TABLE II.
REVEALED INFORMATION OF MIXTURE PASSWORDS. THE USED SETS ARE DIGITS, D, SPECIAL CHARACTERS, SC, AND COMBINATION OF DIGITS AND SPECIAL CHARACTERS, DSC. EC STANDS FOR EXTRA CHARACTERS. GOOD PASSWORDS ARE IN BOLD.

Pw L	Word L+ Nr EC	Mpu D	Mpu SC	Mpu DSC	Mpk D	Mpk SC	Mpk DSC
10	9 + 1	74.2	72.3	72.0	75.2	73.3	73.0
	6,3 + 1	61.7	59.8	59.5	64.3	62.4	62.1
	6 + 4	64.6	56.3	54.8	66.9	58.6	57.2
	5,4 + 1	60.3	58.4	58.1	62.9	61.0	60.7
	5,3 + 2	58.0	54.1	53.4	61.6	57.7	57.0
	4,4 + 2	58.0	54.2	53.5	60.6	56.7	56.0
	4,3 + 3	55.2	49.2	48.1	59.5	53.5	52.4
	3,3,3 + 1	54.0	52.1	51.7	56.0	54.1	53.7
	3,3 + 4	54.7	**46.4**	**44.9**	58.6	50.3	48.8
	3 + 7	60.2	**43.8**	**41.2**	63.2	**46.8**	**44.2**
8	7 + 1	74.5	72.6	72.3	75.5	73.6	73.3
	6 + 2	71.1	67.2	66.5	72.7	68.8	68.1
	5 + 3	68.2	62.2	61.1	70.2	64.2	63.1
	4,3 + 1	63.1	61.2	60.9	65.7	63.8	63.4
	4 + 4	65.9	57.6	56.2	68.3	60.0	58.5
	3,3 + 2	61.8	57.9	57.2	64.4	60.5	59.8
	3 + 5	65.0	54.2	52.4	67.6	56.8	55.0

The difference in revealed information between "unknown" and "known pattern" is a couple of bits based on a comparison of the columns *Mpu* and *Mpk*. However, the amount of revealed information in the *D*, *SC*, and *DSC* -columns show that the use of extra characters from the larger set, yield a much stronger password. The impact is greater, when most of the password characters are extra ones and do not belong to a word-part.

From the above, it can be concluded that the best Mixture passwords consist of a short word (or couple of short words) and many extra characters from a large character set. The short word in our computation was noticed to be a word less than half of the length of the complete password. For instance, for a password of 10 characters, the short words can have a length of 3 and 4 characters.

Word passwords. By pure Word passwords, we mean passwords which contain dictionary words only. The password either contains only one word with the length of the password itself, or several shorter words, with the total length of the words constituting the total length of the password. The analysis of words from one language is divided into two sub-cases.

- W**mod**: the **mod**ified words are used and the placement pattern of the words is unknown.
- W**dic**: the **dic**tionary words are used and the placement pattern of the words is unknown.

It has been shown above that a variation of character placements in each password-design session makes passwords more secure. In the case of Word passwords, the variation is done by using different word lengths. This means that the effect of variation is smaller than in other cases, because there are fewer words than characters in a

TABLE III.
NUMBER OF NORWEGIAN WORDS. THE STATISTICS WERE OBTAINED FROM THE OSLO CORPUS COLLECTION BY NORWEGIAN TEXT LABORATORY, TEKSTLABORATORIET ILN, OSLO, NORWAY.

Word length, l	Number of words, aw
3	3048
4	11145
5	20767
6	29043
7	36590
8	42805
9	45762
10	44956

password. However, we consider that even if the password structure were same, a change in words makes it possible to use different word lengths. For example, *ABussIsWhite* has a different word-length structure than a password with a similar theme password such as *TheTruckWasBrown*. Therefore, we only consider cases in which the word placement pattern in a password is unknown.

In our work, we only compute revealed information entropies when only one language is used, and we decided to use the statistics for Norwegian words. However, the formulae provided are also suitable for other languages.

Computations. The size of the Word password search space is

$$C_{Word} = c_{wo} \prod_{p=1}^{w} aw_p(lw_p), \tag{25}$$

where c_{wo} is the order combination of different words (computed with (19)), w is the number of words, and $aw_p(lw_p)$ is the amount of lw_p -length words. Table III shows the number of Norwegian words with a length of 3-10 letters.

Results. The results for the 8, 10, and 12-character passwords are shown in Table IV. In the *Wmod* case, both forward and reverse transformations are taken into account. The modifications are: all letters are lower case, all letters are upper case, only the first letter is upper case, only the last letter is upper case, the consonants are upper case and the vowels upper case.

The results in Table IV show that the use of original dictionary words does not make passwords secure, especially, if only one or two words are used. The best approach is to use several short words, with different lengths, in one password. Here also, the length of the short word is less than half of the original password length. The use of modified words makes the passwords stronger. However, if the modification is always done in the same manner, the use of modification reduces the password space as much as use of original dictionary words.

It is possible to design strong Word passwords, but not with pure dictionary words. A *good* Word password need to consist of digits, upper case and lower case letters, and special characters. The substitution and rotation should be done differently each time and also differently in each password. A *good* Word password should have at least 12 characters and consists of several short, modified words.

TABLE IV.
REVEALED INFORMATION OF WORD PASSWORDS. GOOD PASSWORDS ARE IN BOLD.

Pw L	Word L	Wmod bits	Wdic bits
12	12	75.1	78.7
	9,3	58.8	66.0
	8,4	57.0	64.2
	7,5	56.3	63.5
	6,6	57.2	64.4
	6,3,3	**43.7**	54.5
	5,4,3	**41.3**	52.1
	4,4,4	**42.9**	53.7
	3,3,3,3	**33.4**	47.7
10	10	75.0	78.6
	7,3	59.1	66.3
	6,4	57.6	64.7
	5,5	58.2	65.3
	4,3,3	**45.1**	55.8
8	8	75.0	78.6
	5,3	59.9	67.1
	4,4	60.0	67.1

The modified Word passwords look like Mixture passwords, but, because they are constructed from dictionary words, the underlying word pattern makes them weaker than Mixture-words. We do not have statistics specifying which letters are modified and by which other character, but it can be assumed that substitution by people follows the certain pattern.

The number of dictionary entries is small compared to the total size of the password search space. However, the actual size of word-sets used in passwords might be even smaller. People have tendency to use theme words [2], [7] such as name of the sport teams, food, and animals. The size of such themes is very small and the use of words only from one theme makes password design process very weak.

III. PASSWORD FORMATION GUIDELINES

A good password is complex, but nonetheless easy to remember [8]. The password policy should be such that it combines individual password design processes, while helping users to generate secure passwords with their own methods. In Section II, we showed that *good passwords* can be created in each category, if there are enough variations in pattern and character. Variations provide good defences against attacks based on language structures e.g. fast dictionary attack in [1].

In order to design *good passwords*, we propose the following guidelines.

Non-word password design.

1) A password should be longer than 8 characters.
2) Use characters from all character sets, so that more characters come from the large character sets than from the small sets.
3) Vary the number of characters from each set in each construction session.
4) Vary the patterns of character placement.

Mixture password design.

1) A password should be longer than 10 characters.
2) Use either one short, modified word and many extra characters or several short (not the same length), modified words and a few extra characters from large character set.
3) Avoid using same theme.

Word password design.

1) A password should have more than 12 characters.
2) Use many short and modified words.
3) Avoid using same theme.
4) Use variation when modifying.
5) Use different languages and language combination when designing a new password.

Note that the length of a short word is less than half of the length of the password.

IV. Related Work and Discussion

When designing passwords and password policies, users should also develop an understanding that passwords are not only vulnerable against brute-force attack, but also against much more sophisticated attacks. A common denominator of the latter is *password search space reduction.* After reduction, the attacks, be they brute-force or dictionary attacks in smaller search spaces, become faster and therefore constitute a far more serious threat.

In our study, the reduction of password search space is computed from the adversary's acquired knowledge on the password policy and the password-generation process. More sophisticated methods for password search space reduction are presented in [1], [9]–[11].

Trostle [9] describe timing attacks against the trusted path mechanism. Only a few trials were needed to obtain the length of the password with the first attack type. The second attack continued to obtain leakage and was able to reduce the strength of a password by 2-3 bits per character.

In a study of Song et al. [10], the use of keystroke latency information in timing attacks toward passwords in the Secure Shell was analyzed. Typing patterns were estimated and, with the help of latency information, the strength of a password was reduced by 1.2 bits per character pair.

In [1] Narayanan and Shmatikov reduced the password search space by using Markov modelling techniques of natural language processing. They claim that the distribution of letters in easily remembered passwords is similar to the distribution of letters in the users' native language. Based on this concept, they combined an algorithm which enables a fast dictionary attack. First Markov filters are used to reduce the size of the password search space, and then, the remaining search space is efficiently enumerated and in the final stage, time-space trade off techniques are used to conduct a fast dictionary attack.

Markov filters and English language structures were also in use when Zhuang et al. [11] presented their keyboard acoustic emanation attack. They recorded 10 minutes of English text and were able to recover 96% of the typed characters.

In the NIST Special Publication on Electronic Authentication Guidelines [12], the use of three different password policies were evaluated and the minimum password guessing entropies, versus password length for each policy, were estimated. Compared to NIST evaluation, we used the password analysis based on textual meta-information, and went one step deeper, by studying human password design processes.

More password policies and their relationship to user memorability, password entropy and password change frequency were simulated and analyzed by Shay et al. [7]. They noted, as had many before [13], [14], that if a password policy does not require sufficiently complex passwords, users' passwords are in danger of being cracked. If a policy requires overly complex passwords, users may have problems to recall them and therefore may write them down.

Password generation process and structure were studied in [5], [6]. MySpace phishing attack analysis [6] showed that 65% of passwords were 8 characters or less long and 81% of passwords were alphanumeric, which, in most cases, contained lower case letters with a single digit at the end. In one third of the cases, the digit was 1. Brown et al. in [5] found that 65% of passwords were generated from information relating to the user himself. Almost one third of these were names. The next largest groups were dates, and ID and phone numbers. Three quarters of the passwords contained the full information. There was only a modification of the information in less than 5% of the passwords. These findings suggest that users generate passwords with minimum length and structure and even the content is familiar. The users of these studies cited above, would benefit from our password policies.

Based on our analysis, we are able to provide concrete guidelines for password policy construction in each password category: Non-Word, Mixture and Word password. This allows users to develop their own password style and still create memorable passwords, while keeping the structure of passwords complex enough to ensure security. Passwords constructed according to guidelines are strong, even if these guidelines are available to the adversary.

An educational tool [15] based on the findings and guidelines of this paper, has been made to help users measure the quality of their password and also to design stronger passwords.

V. Conclusion

People *are* able to design memorable passwords, especially if they can use their own password-designing processes. These processes can produce passwords which we have divided further into three categories: Non-word passwords, Mixture passwords, and Word passwords. Within these categories, we have provided formulae and

computations of effective password space for many different password policies. Based on this analysis, we have compared how effective password space is affected by policy decisions. We have computed how valuable a knowledge of password policy is for an adversary, in terms of reduced password entropy and consequently, a reduction in the necessary search space. Based on computations of typical password sizes (8-14 characters), we have provided guidelines for password policy construction. These guidelines identify policy statements that help to reduce the loss of password entropy.

ACKNOWLEDGEMENTS

The authors are grateful to the anonymous reviewers for their careful reading and valuable feedback. This work is supported by the Research Council of Norway, grant 158777, Authentication in a health service context.

REFERENCES

[1] A. Narayanan and V. Shmatikov, "Fast dictionary attacks on passwords using time-space tradeoff," in *Proc. of 12th ACM conference on Computer and communications security*, 2005, pp. 364–372.

[2] F. Monrose and M. K. Reiter, "Graphical passwords," in *Security and Usability: Designing Secure Systems that People Can Use*. O'Reilly, 2005, ch. 9, pp. 161–179.

[3] S. Gaw and E. W. Felten, "Password management strategies for online accounts," in *Proc. of Symbosium On Usable Privacy and Security*, 2006, pp. 44–55.

[4] E. Gehringer, "Choosing passwords: security and human factors," in *Proc. of International Symposium on Technology and Society*, 2002, pp. 369–373.

[5] A. Brown, E. Bracken, S. Zoccoli, and K. Douglas, "Generating and remembering passwords," *Applied Cognitive Psychology*, vol. 18, pp. 641–651, 2004.

[6] B. Schneier, "Crypto-gram newletter: Real-world passwords," http://www.schneier.com/crypto-gram-0612.html, December 2006.

[7] R. Shay, A. Bhargav-Spantzel, and E. Bertino, "Password policy simulation and analysis," in *Proc. of ACM workshop on Digital identity management*, 2007, pp. 1–10.

[8] P. Cisar and S. Cisar, "Password - a form of authentication," in *Proc. of 5th International Symposium on Intelligent Systems and Informatics*, 2007, pp. 29–32.

[9] J. Trostle, "Timing attacks against trusted path," in *Proc. of IEEE Symposium on Security and Privacy*, 1998, pp. 125–134.

[10] D. X. Song, D. Wagner, and X. Tian, "Timing analysis of keystrokes and timing attacks on ssh," in *Proc. of 10th conference on USENIX Security Symposium*, vol. 10, 2001.

[11] L. Zhuang, F. Zhou, and J. Tygar, "Keyboard acoustic emanations revisited," in *Proc. of 12th ACM conference on Computer and communications security*, 2005, pp. 373–382.

[12] W. E. Burr, D. F. Dodson, and W. T. Polk, *Information Security: Electronic Authentication Guideline*. NIST Special Publication 800-63 Version 1.0.2, 2006.

[13] C. Kuo, S. Romanosky, and L. Cranor, "Human selection of mnemonic phrase-based passwords," in *Proc. of 2nd symposium on Usable privacy and security*. ACM Press, 2006, pp. 67–78.

[14] M. Sasse, S. Brostoff, and D. Weirich, "Transforming the "weakest link" - human/computer interaction approach to usable and effective security," *BT Technol*, vol. 19, no. 19, pp. 122–131, 2001.

[15] K. Helkala, "An educational tool for password quality measurements," in *Proc. of Norwegian Information Security Conferences (Norsk Informasjonssikkerhetskonferanse, NISK)*, November 2008, pp. 69–80.

BIOGRAPHIES

Kirsi Helkala is a doctoral candidate in information security at Gjvik University College, Norway. Her research topic is personnel authentication.

Einar Snekkenes is professor of information security at Gjvik University College, Norway. He has published on such topics as cryptographic protocol analysis, privacy, social engineering, biometrics, authentication, testing and smart card side channel attacks. His research interests include information security and risk analysis.