

APPENDIX A

How to choose a password that is not easily guessable

The programs that try to guess passwords (or the attacker of a machine) do not try all existing passwords, they only try a large number (10^8) of "frequently used" passwords. So if you stay out of this search space you are safe; to do so you can follow the following guidelines:

First, here is what you should NOT do:

- Don't use your login name in any form (as-is, reversed, capitalized, doubled, with a prefix, with a suffix, etc.).
- Don't use in any form your first or last name and, more generally, any information easily obtained about you. This includes license plate numbers, telephone numbers, social security numbers, the make of your car, the name of the street you live on, the name of your spouse or of your children, etc.
- Don't use a word contained in any dictionary of any language, spelling lists, or other lists of words (acronyms, sequences of letters like 'abcdef' or 'qwerty', place names, car names, cartoon heroes, etc.).
- Don't use a password shorter than six characters or with only alphabetic characters or only digits.

Then, here is what you should do:

- Do use a password with mixed-case alphabets, digits, punctuation.
- Do use long passwords (with more than 6 characters).

Important note: please remember that each operating system impose its own restrictions:

- UNIX: you can use all printable characters, case IS significant and only the first 8 characters will be used, so in the password 'computer+3,Z' only 'computer' is significant and the remaining characters will be ignored.

- VM: you can use only alphanumeric characters, case IS NOT significant and the maximum length is 8.
- VMS: you can use all printable characters, case IS NOT significant and you can use long passwords (up to 32 characters).

Finally, here are some methods for making passwords:

- Choose a line or two from a song or poem, and use the first letter of each word. For example, 'In Xanadu did Kubla Kahn a stately pleasure dome decree' becomes 'TXdKKaspdd'.
- Alternate between one consonant and one or two vowels, up to eight characters, do use mixed-case. This provides nonsense words that are usually pronounceable, and thus easily remembered (ex: 'roUtboo', 'quADpop', and so on.).
- Choose two short words (or a big one that you split) and concatenate them together with a punctuation character between them (or a digit if you can only use alphanumeric characters). For example: 'dog+F18' or 'comP7UTer'. Note that 'dog', 'F18' or 'computer' are in dictionaries but as the passwords use punctuation or digits, mixed-case character, they are really hard to guess.

Remark: if you use mixed-case characters, do not use the following methods:

- all lowercase or all uppercase
- only the first or the last character in uppercase
- only vowels in uppercase
- only consonants in uppercase.