Generating Good Passwords (2):
Bytes Interactive Password Generator

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Last time I asked, “What’s a good password?” and discussed a Web-based service for creating random passwords. This time I’m looking at the “Bytes Interactive Password Generators”<http://www.goodpassword.com/index.htm>.

This site provided two types of password: the random and the “Leet.”

The Leet password generator asked for a phrase of eight or more words. I gave it the classic “The quick brown fox jumped over the lazy dogs” and it created “+q8Fjo+1d” with a “Password Pattern” of “LclCclLlc.” The symbols in the password pattern are supposed to help the user remember how to transform the first letter of the passphrase into the password. The meaning of the symbols is as follows:

- C Upper Case Character
- c Lower Case Character
- l 1st Leet Character Equivalent
- L 2nd Leet Character Equivalent

The “l” and “L” symbols refer to certain letters that have two different substitution codes for the “elite” (leet) alphabet; thus the first Leet character in this transposition cipher for A is @ and the second is 4.

```
A  @   4
B  8
C  [   (D  D
E  3
F  F
G  6   9
H  #
I  !   1
J  J
K  K
L  1
M  M
N  N
O  0
P  P
Q  Q
R  R
S  5   $
T  7   +
```
The Web site authors state, “To remember your 1337 Password you need two keys, first the pass phrase and second the password pattern. This pattern will indicate whether the password characters are either upper or lower case, or a Leet Equivalent. The pass phrase one should try to memorize or at least know what book, page and location on the page the phrase was taken from. The password pattern is harder to remember so we recommend writing it down or using our Password Recovery Feature.[sic] by creating a cookie from our web site to remember the pattern for you. Try the Password Recovery Feature.”

As you may imagine, I am not keen on the generated passwords, since they do not strike me as particularly easy to remember unless the user knows the hacker alphabet by heart. Perhaps this generator is intended for people who are or have been script kiddies, hacker wannabees or otherwise involved in the criminal hacker subculture.

However, the idea of writing down the password _pattern_ (not the password or the passphrase) or of storing the pattern in a cleartext cookie on an unencrypted drive does _not_ strike me as a significant security risk in the absence of the original passphrase. The pattern alone is useless without the passphrase.

Next time (the last in this short series), I’ll introduce a random-password generator based on a classic paper in the computing literature.

***


***

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.gradle.norwich.edu/infoassurance/> and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2007 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.