Creating Strong and Easy to Remember Passwords

14 October 2022

G.A.Jennings

Abstract

Presented here is a simple technique for passwords that are both strong and easy to remember. Seriously.

Introduction

Think in terms of tokens. Start with short character sequences of a particular format, and make your passwords from a number of these tokens. Each token will be different, short and memorable. Concatenate several tokens together and you have your strong, unique, remember-able password.

For my examples I'll use four disparate tokens. These are guidelines. People should make up their own token system, but this system is as good as any and better than most.

Tokens

First token is a non-word word, which is a sequence of letters that is pronounceable like word but is not a word (NWW). Second token is a number (NUM). Third is punctuation (PUN).

From those you make a password root. Once chosen, there will be a forth token of your choosing which will be used to make a different password for each account you want a password for.

Here is a notation for the tokens:

```
[NWW]
[NUM]
[PUN]
```

Here are some example tokens (with the token category obvious):

```
Foobey
Bletch
411
187
!
?
```

(The fourth token comes later.)

To make this work you would make up tokens that are unique to you. The non-words from any milieu in your brain, numbers from your surroundings or from any set of related numbers (or random), and your favourite punctuation character. (Some of you might like to use hexadecimal or octal numbers.)

Order

Once you have some tokens you need to order them any way you like. The result will be a strong and easily remembered unique sequence of characters that can not be guessed or cracked by any algorithm (before we all die and turn to dust anyway).

Just two examples will demonstrate:

```
[NWW][NUM][NWW][PUN]
[PUN][NWW][NUM][NWW]
```

Just pick the quantity and order you like that you can remember. Those examples show a minimum number of tokens for anyone to come up with something fairly strong. Larger brain capacity? Then use more tokens. But those minimums really are sufficient. (And not yet complete.)

Here are a couple of these types of passwords:

```
Foobey9Bletch$
42Bletch!Foobey
```

Pretty Good Passwords (as this technique can be called). The result should be "pronounceable" as well (i.e., "Foobey Nine Bletch Dollar").

Finalize

Once you have your password root, one more token is needed, one to use for each account, and unique to you. Perhaps, one or two capital letters, related in some way to the account, prepended or appended:

```
Foobey9Bletch$A
Foobey9Bletch$P
```

And there you have it. An easily remembered, strong, non-guessable, non-crackable password.

One last thing. One can use the password root (`Foobey9Bletch` for example) by itself for all accounts that do not have a website login, such as FTP accounts or mail accounts (that are not Yahoo, Gmail, etc.). Those being the same is pretty safe as such accounts do not have published or public interfaces.

But surely, Yahoo and Google track their mail website submit forms for automated attacks, right? Surely. (They'd be negligent if not; they ain't Wordpress...)