Strong Passwords and Password Managers

By Kevin Birk
CTISO, ENMU-Ruidoso

What is a 'strong' password?

A password is a sequence of characters that is used to secure access to a file, folder, or system. Most users pick sequences that spell out easily remembered phrases, acronyms or numbers. These however are not 'strong' in the sense that they can be fairly easily broken with brute force dictionary attacks which run through common numerical sequences, words and phrases.

To make matters worse, if a password is reused between different sites and is exposed through a hack or a leak, it may expose the user to unauthorized access on any other sites in which the password is used. Therefore, it is important for the user to secure each login with a unique and strong password.

These days, a strong password is considered to be at least 12 characters long using a mix of case-sensitive alphanumeric and special characters. Consider the following examples of weak and strong passwords:

Weak:

12345678

userpass

ryan709mechem

kevinBirkPass

Strong:

1Y7eqeEwLMBBnJOF

2K1s!KKNz0pX%xc#

B1z4ff4ir5Ru!

@m3ch3m4nd$ud3rth

The weak examples above utilize easily guessed numerical sequences and easily guessed words. Passwords are even weaker when they contain elements of their corresponding user name as with 'ryan709mechem' or 'kevinBirkPass'. Additionally, the shorter the password is, the fewer tries a password breaking program will need to ensure a successful guess.

The strong examples utilize either entirely random sequences of characters, or utilize somewhat recognizable words or phrase along with a high degree of alpha-numeric substitution. Since the passwords are very long, they become harder to guess with each added character. Consider the vastly higher number of combinations between 40^8 and 40^16.

Of course, the trouble with complex passwords is that they are difficult or impossible to remember, a task made much more complicated when needing a unique one for each login. This is where password manager programs come in.

Security Questions

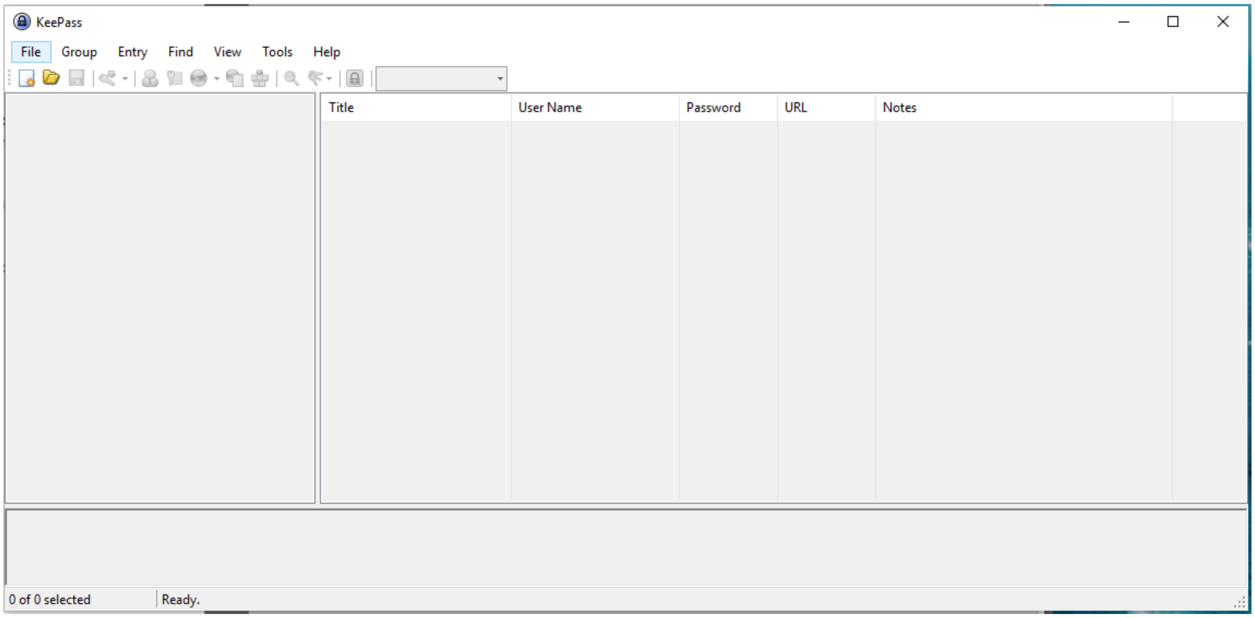
Oftentimes a website will ask you to create security questions to help recover your password or to verify your identity on login. We recommend creating fake answers unique to each website as a way to mitigate the risk of your security question data being hacked, leaked or guessed on another site and being used to recover logins on the remainder of your sites. If the sites have the same security question answers then it may become very easy for a would-be intruder to steal your login/access credentials.

Password Managers

Password manager are programs that help you to store your logins and generate strong passwords. Some examples of commonly used password managers are LastPass and KeePass. Most modern browsers such as Google Chrome, Mozilla Firefox and Apple Safari offer limited password manager services as well. Our password manager that we recommend working with is KeePass, a light, freeware program that makes it easy to store and keep track of all your logins.

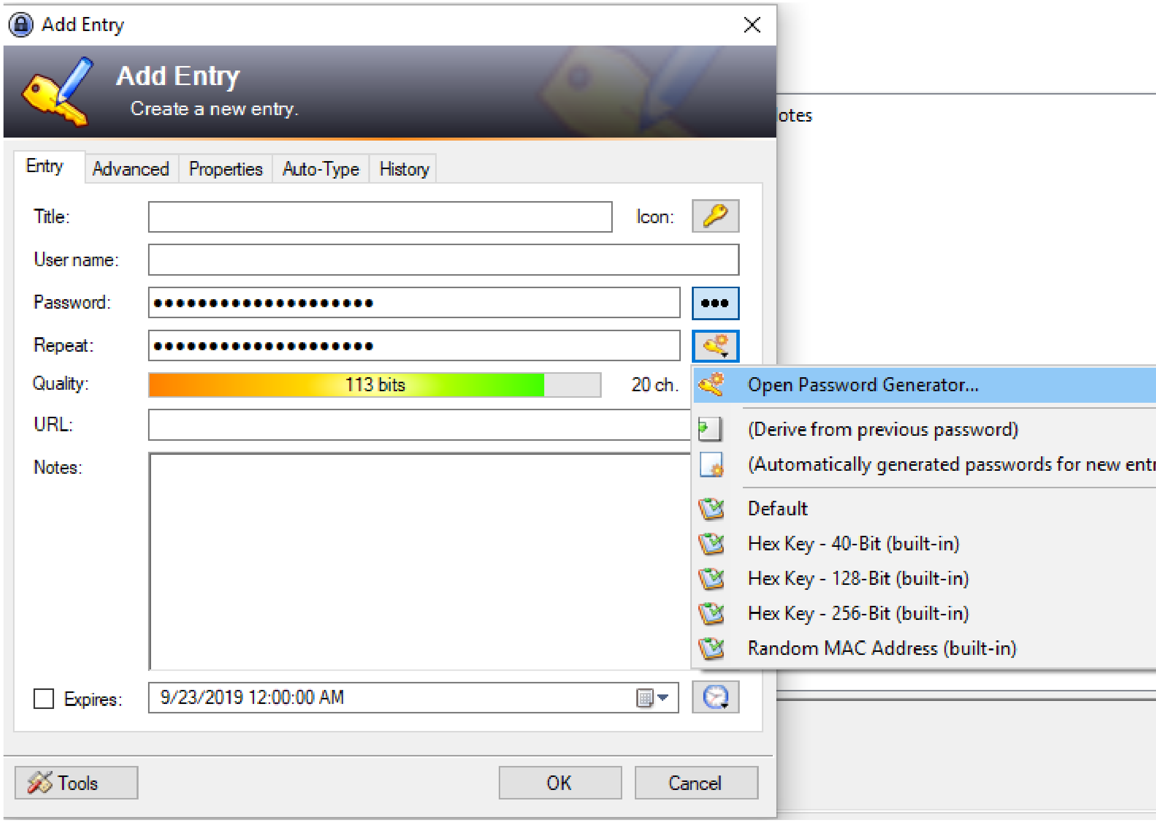
Use the following steps to create a KeePass Database for yourself or your department:

1) Open KeePass



2) Click 'New' to create a new password database file.
3) Name the password database file and choose a location to save it to
    a. I recommend locating the database in a cloud backed-up folder, or into a departmental share folder. This will help ensure that you do not accidentally delete your password database file.
4) Create a master password or key file
    a. Create a strong password by hand, making it at least 12 characters long, and utilize a high degree of randomness or alpha-numeric substitution.
5) Choose a name for the database
    a. I recommend something like 'myDept logins', inserting the name of your department for 'myDept' as appropriate.
6) Delete the default folders within your new password database
7) Create new folders for each group of logins
8) Create entries for each login as needed
    a. Give the entry a title
    b. Enter the username for the login
    c. Give the login a password
        i. Either enter a password of your choice, or have KeePass generate one for you

ii. To generate a password, click the key icon to the right of the “Repeat” field:


Add Entry
Add Entry
Create a new entry.
otes
Entry
Advanced
Properties
Auto-Type
History
Title:
Icon:
User name:
Password:
Repeat:
Quality:
URL:
Notes:
Open Password Generator...
(Derive from previous password)
(Automatically generated passwords for new entr
Default
Hex Key - 40-Bit (built-in)
Hex Key - 128-Bit (built-in)
Hex Key - 256-Bit (built-in)
Random MAC Address (built-in)
Tools
OK
Cancel

Password: ••••••••••••••••••••

Repeat: ••••••••••••••••••••

Quality: 113 bits 20 ch.

□ Expires: 9/23/2019 12:00:00 AM

1. Select the password options as desired, hit ‘Ok’
2. The new password generated will be filled into the password field

d. Enter the login URL of the site to help remember what it is for

e. Add Notes as appropriate

i. This can be a handy place to store any ‘security question’ answers, as well as an confirmation codes or other identifiers/passphrases used in your login

f. Hit Ok to save the entry

9) For more information on usage of KeePass, please see the KeePass First Steps guide and the KeePass online manual.