Sun City Summerlin

Computer Club Seminar

Password Management using

KeePass

Jeff Wilkinson

Seminar Agenda

- Introduction
- Why Should I use a password manager?
- What is KeePass
- Why use a different password on each site?
- Strong passwords
- How to download and install KeePass
- How to enter data in KeePass
- Questions and Discussion

Why Should I Use A Password Manager

Without a way to manage passwords, the tendency is to pick less secure passwords that are easy to remember

- **Installing a password manager is one of the most important things you can do to help keep your data safe and secure.**
- ***KeePass*** is a password database/manager that helps manage passwords in a safe encrypted database accessible with a single password.
- **Sticky notes leave a paper trail and are insecure**
- **You can print out your password database if you like and securely store it.**

What is KeePass

- KeePass is a FREE open source password manager which helps you manage your passwords.
- KeePass is portable - for PC (Windows, Linux, Mac OS X), with Apps available for Android, iPhone, iPad, and more.
- KeePass database files are encrypted. KeePass encrypts the complete database, i.e. not only your passwords. The user names, notes, etc. are encrypted, too.
- KeePass uses a Federal government standard encryption method that is approved by the National Security Agency (NSA) for top secret information.

What is KeePass

- Locked file stored on computer or portable file stored on memory stick
    1. Iphone – MiniKeepass
    2. Android Aps – KeePass2Andoid
    3. Stored in cloud – Google Drive, iCloud
    4. Notes on security questions which you answered long ago and may have forgotten
    5. Subscription renewal dates and term
    6. Bank Acct numbers, routing numbers
    7. URL of exact page you wish to access

- Accessible from Cloud – like Google drive so effectively sync all your devices

Why Use A Different Password On Each Site

A 2013 poll of 1805 adults aged 16 and over, discovered that 55% of them used the same password for most – if not all websites.

Why you should use a different password on each site:

- Use of the same password on multiple sites or use the same password over and over
  - If a Site is hacked – user database compromised
  - User name
  - Password or a portion of it
  - Password hints

  Use a different password for each of your important accounts, like your email and online banking accounts. Re-using passwords is risky. If someone figures out your password for one account, that person could potentially gain access to your email, address, and even your money.

Strong Passwords

You should use different password for each account. If you use only one password everywhere and someone gets this password you have a problem... A serious problem. The thief would have access to your e-mail account, website, bank account, etc.

Here is a typical scheme of password generating.

- **First thing that comes to most users' minds is to use our pets' names, car model or the word “password”. Surely, you are the only person who has red Ford 2008, a dog called Foxy and a password “Password”**

- **The combination of numbers like – 12345,246810,654321 etc.**
- **Your favorite movie or a book title, the name of the country or color – a frequent phenomenon.**
- **Strong passwords contain a mix of letters, numbers, symbols**
  -

Strong Passwords

- An eight-character password with numbers, symbols and mixed-case letters is harder to guess because it has 30,000 times as many possible combinations than an eight-character password with only lower case letters.

https://password.kaspersky.com/

- Test your password strength – use a similar password

- **Sam321** -> Your password will be brute forced with an average home computer in approximately 10 minutes

- **XG261268@!er_23** -> Your password will be brute forced with an average home computer in approximately 233 centuries

Download, Setup and First Time Use

Download from http://keepass.info/download.html

Download V2.34 Professional Edition Installer

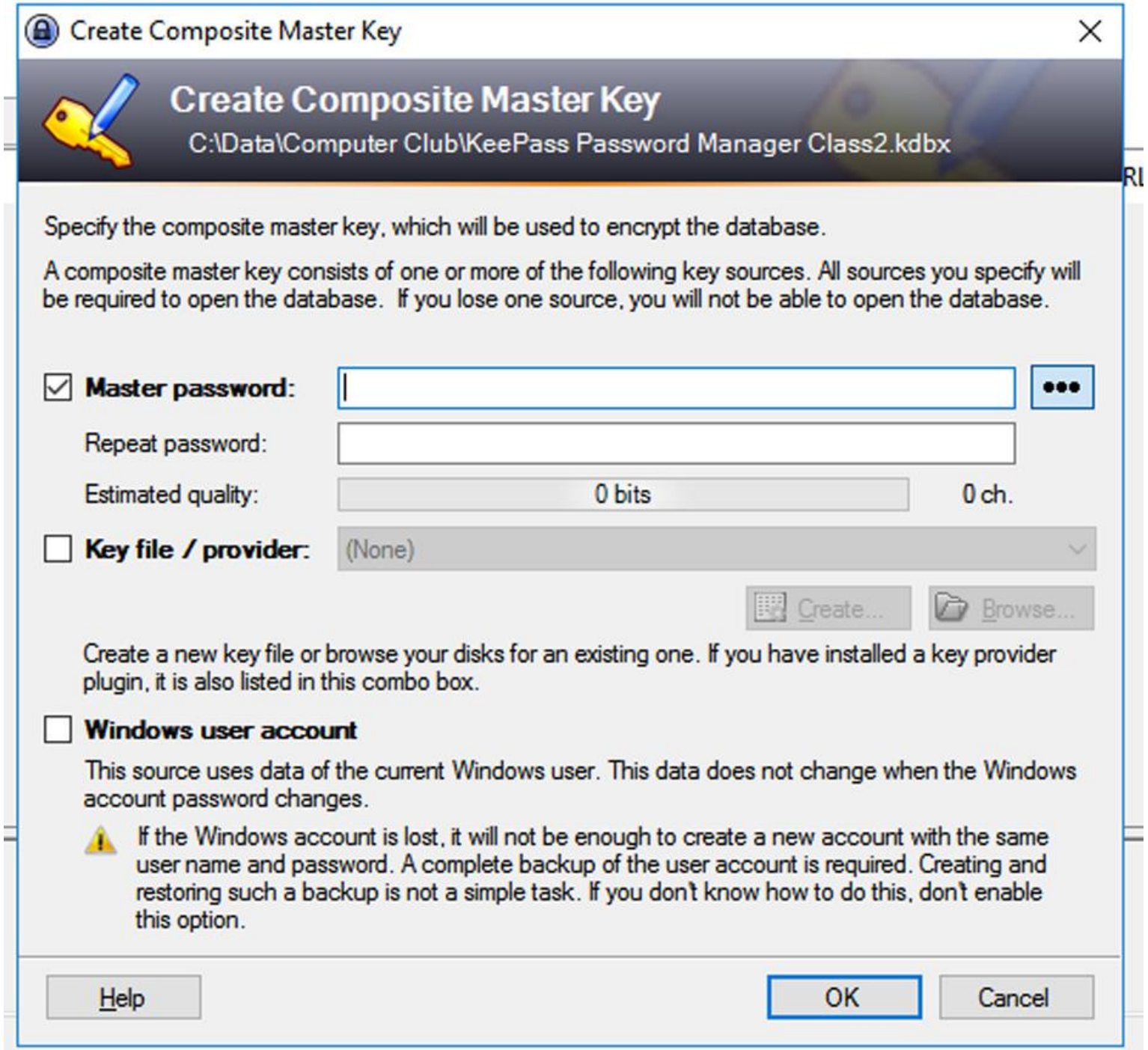
Installation:

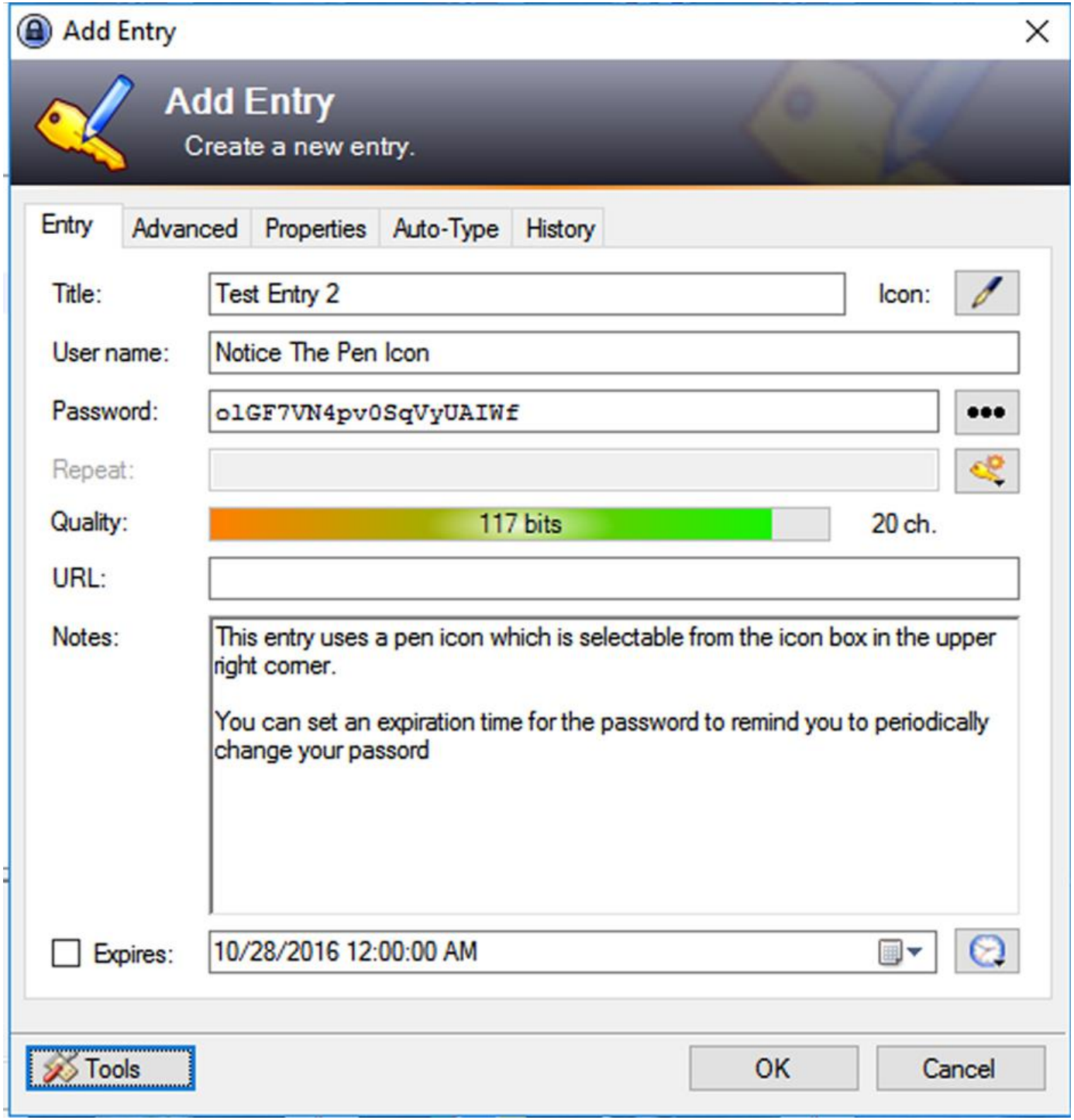
To install KeePass, run the KeePass-2.xx-Setup.exe file and follow the wizard.

Allows user to select file location – drive and folder, Google drive folder

You only have to remember one single master password or insert the key-disk to unlock the whole database. The databases are encrypted using the best and most secure encryption algorithms currently known (AES and Twofish).

- – should be **strong** as it's the only one protecting your other entries


Create Composite Master Key
Create Composite Master Key
C:\Data\Computer Club\KeePass Password Manager Class2.kdbx
Specify the composite master key, which will be used to encrypt the database.
A composite master key consists of one or more of the following key sources. All sources you specify will be required to open the database. If you lose one source, you will not be able to open the database.
Master password:
Repeat password:
Estimated quality:
0 bits
0 ch.
Key file / provider:
(None)
Create...
Browse...
Create a new key file or browse your disks for an existing one. If you have installed a key provider plugin, it is also listed in this combo box.
Windows user account
This source uses data of the current Windows user. This data does not change when the Windows account password changes.
If the Windows account is lost, it will not be enough to create a new account with the same user name and password. A complete backup of the user account is required. Creating and restoring such a backup is not a simple task. If you don't know how to do this, don't enable this option.
Help
OK
Cancel


Add Entry
Add Entry
Create a new entry.
Entry
Advanced
Properties
Auto-Type
History
Title:
Test Entry 2
Icon:
User name:
Notice The Pen Icon
Password:
o1GF7VN4pv0SqVyUAIWf
Repeat:
Quality:
117 bits
20 ch.
URL:
Notes:
This entry uses a pen icon which is selectable from the icon box in the upper right corner.
You can set an expiration time for the password to remind you to periodically change your passord
Expires:
10/28/2016 12:00:00 AM
Tools
OK
Cancel

When you open the database with your newly created strong password, you have a number of options which you can choose or just use the default settings.

General Tab

Name: Under the general tab, name your password database

Database Description: You can enter a description of your password database

Default Username: You can have a default username appear each time you add an entry – I don't use this as I have a unique username on most sites

Database Color: You can choose a database color – this only appears to work on initial creation of the database. I use the default.

Security Tab

Choose encryption algorithm – I use the default

Compression Tab

None or Gzip – Choose Gzip

Recycle Bin

Select this option for second chance if you accidently delete an entry

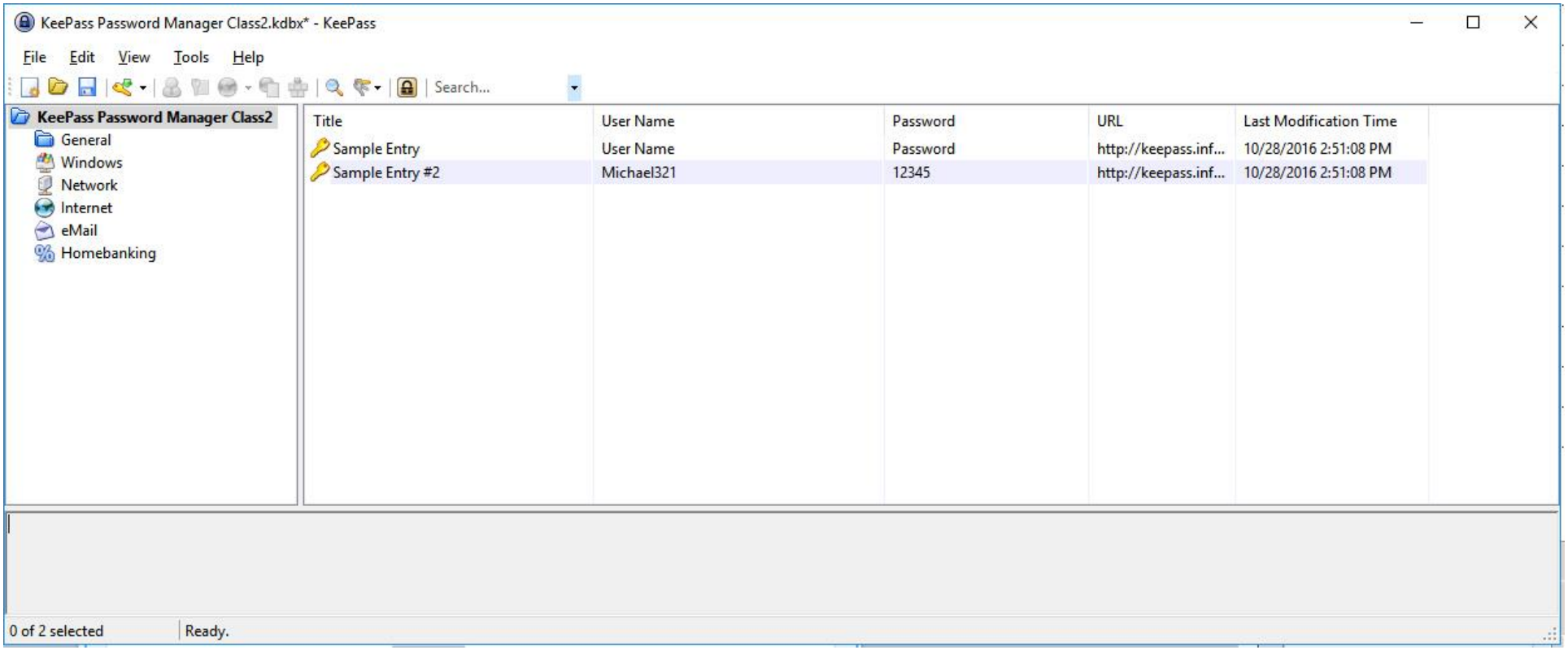
Advanced Tab

Templates Group: You can create a template with data already entered – i.e. employee data where all company name, department, location etc. doesn't change

Master Key Change – you can set number of days to be notified of recommended or required password change of the master password

How Do I Use KeePass

You can print you database passwords at any time to keep a hard copy in a safe location



Info you can keep in remarks:

Cox or Century Link phone number, locations, terms of subscription, when and how you paid, member number(s), banking Info – routing #, account(s) numbers, answers to security questions

Remarks are also encrypted

Using entries

You got the new entry in the password list now. What can you actually do with it now? Right-click on the entry.

You have several options now. You can copy the username of the entry to the Windows clipboard. When you've copied it, you can paste it into any other program of your choice. The same works for copying passwords.

Alternatively, you can drag&drop fields into other windows. To see an example of how this works, see this page: Drag&Dropping Fields.

How Do I Use KeePass

Auto Type -> By default, the sent keystroke sequence is **{USERNAME}{TAB}{PASSWORD}{ENTER}**

KeePass can open the URL you specified. To do this, just click *'URL(s) - Open URL(s)'* in the context menu. KeePass will start the default browser and open the specified URL.

Questions & Comments