KeePass

Keep your passwords SAFE

John Steele

What we will cover

- What is the problem with passwords
- How complex do they need to be
- How can they be stored safely
- How can they be used easily
- How can they be used on multiple computers

What is the problem

- Passwords (and additional security features) prevent unwanted access to your data
- Use of the same password for more than one site is easy but
  - One compromise could then expose all related sites to exploit
- Simple passwords can be “brute force” attacked
  - Need to be long and complex
- Complex passwords may be difficult to remember and type accurately

Password complexity

- Password length is often restricted by the site
  - Minimum length may be enforced (Good)
  - Complexity (use of Letters, Numbers and punctuation) make brute force attacks less likely
  - Some sites may thwart good passwords
    - Maximum length may be limited (bad)
    - Character set allowed may be constrained
- More complex schemes may be used e.g.
  - Pick 3rd,7th, and 14th character from password
  - Select 3rd, 5th, and 2nd character from pull down list

Storing Passwords

- Use of unique passwords for each site means that they are impossible to remember!
  - Schemes that use suffixes to a common password root are well known to attackers
- Saving them in a text file or spreadsheet is OK unless someone can get at your computer or compromise your defences and copy your file
  - A spreadsheet can be protected by a password but recent versions of Excel are relatively trivial to break
    - after version 2003 and before version 2013

Ease of use

- Long and Complex passwords are more SECURE but DIFFICULT to type!
  - Error prone and take time and may need to be typed several times if sites time out
- Copy and paste from a spreadsheet often works but some sites deliberately prevent it
- There needs to be a better way
- Password manager – one master password
  - **KeePass**

KeePass - Introduction

- KeePass is a Password Manager
  - It will securely hold user names and passwords and any other related data you wish
- KeePass is Free and Open Source
  - See <Website> for download link and more details
- Two versions are available and maintained
  - Version 1 and Version 2
    - These have different options and features
  - There is a “portable” version that can be run without installation

KeePass – Introduction (2)

- KeePass is a Windows program
  - Version 2 depends on having the .NET framework
  - Can be run successfully on Linux or Apple Mac computers with third party programs or packages
- Ports are available from third parties for other platforms (see web site) including
  - Android
  - Apple iOS

KeePass Basics

- A KeePass database is held in a standard file that can be copied, and backed up as part of a standard backup regime
- The Database is encrypted securely and is unlocked by one or more of the following:
  - Password – this should be of appropriate strength
  - Keyfile – a specially built file that should NOT be kept with the Database file
    - Keep on removable media is recommended
  - Windows Account – **NOT RECOMMENDED**

How do I create a Database

- Run KeePass (Version 2 assumed)
- Click Menu → File → New
- Accept default file name [NewDatabase.kdbx] or enter a new one
  - The extension defaults to .kbdx
- You are shown a dialog box to create the password
  - You can type in a master password
  - You can create a Keyfile or use an existing one
  - You can add the Windows Account **(DON'T)**

What can I do now?

- You can open the database by
  - Opening KeyPass and using that to open the file
  - You can double click on the database file
- You will see some default groups and two sample entries
  - Groups are used to organise your records
    - New groups can be created
    - Entries can be dragged between groups
    - Existing ones deleted
      - Note that entries contained in Groups are also deleted
      - Deleted groups or entries go into a Database recycle bin

What can I do next?

- You can add a Windows Title to the entry
- You can add/change the User name and password fields
  - Note that the password has to be entered twice unless you reveal the password (use the …)
  - The password is the one that will be used to log in to the site – more later
- You can add/change the URL field
  - The URL field is used through the World icon on the KeePass toolbar to open the site

Additional fields

- KeyPass can also store additional items of information in each entry - Custom Fields
- Custom Fields are defined in the Advanced Tab
  - Fields have a Name and a Value
  - Once defined the same name can be used in other entries
  - Values are strings
    - Ticking the in memory protection hides the value everywhere except when editing and encrypts the value held in the computer memory
  - You can also add Attachments – use sparingly

What is all this data for?

- Click on the link Icon in the KeePass toolbar
  - The Web site will open (using the URL field)
  - Navigate to User/Password page (if necessary)
- Automatically login using the keyboard keys CTRL+ALT+A
  - KeePass will identify the Web site page via its Title
  - KeePass will Auto Type the User name and Password into the fields and **automatically log into the site**
- We will look at how this happens and how to make it happen in more complex cases

More on Passwords

- When you create a new entry KeyPass creates a RANDOM password.
  - You can also manually type the password into the password field on the KeePass entry tab
- You can control
  - how long this Random password is
  - How complex this is
  - Give the password an expiry date
- You can create a new password in KeePass
  - click on the Generate password button

Generate Random Password

- Clicking on the Generate Password shows a popout dialog box including Generate Password
- A new box opens showing the options available. These are the main options:
  - Length – unless you know you may need to manually enter it make it long (15 to 20)
  - Character set – choose characters that are permitted by the site.
    - Note you may need to experiment as many sites do not tell you their rules
  - There are even more options if this is not sufficient

AutoType – Login to a site

- CTRL + ALT + A will by default initiate Autotype
- Autotype will by default inherit a Group Autotype sequence and type it into the site using the field values (assumes tha the focus is on the User ID field on the web page)
  - <username><tab>password><enter>
- This can be overridden on each entry
  - Within each entry you can select individual Window Titles to be matched (with wild cards)
  - This helps where there is a sequence of login screens

More on Autotype

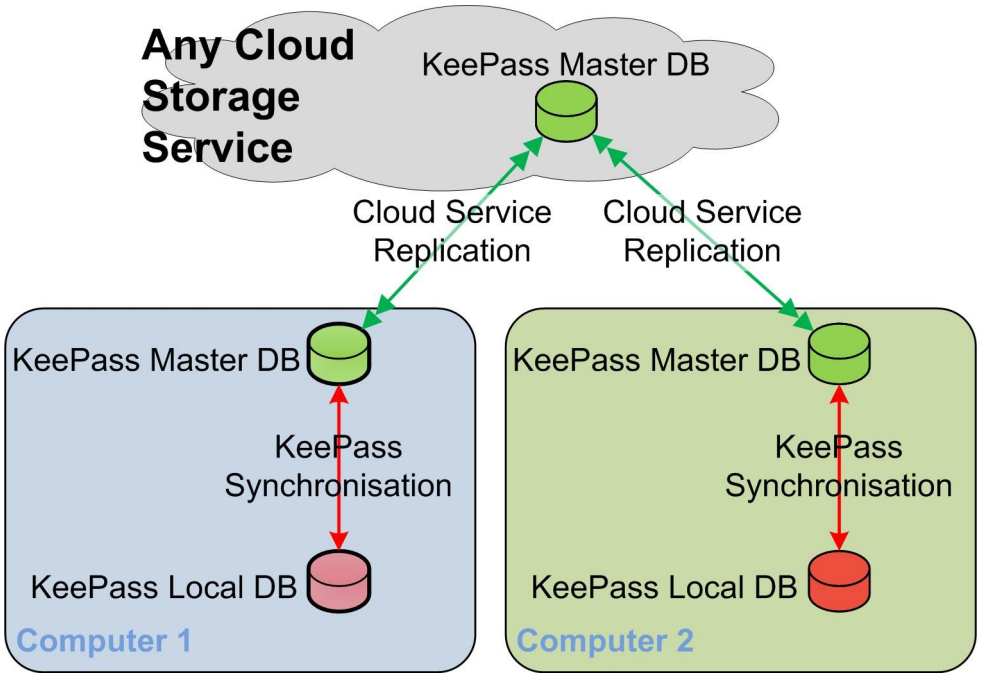
- Autotype supports many options in addition to Username and password fields
  - PICKCHARS enables the selection of “pick characters 3,5 and 11 from your password”
    - {DELAY=250}{PICKCHARS:PIN #:ID=1,C=3} {PICKCHARS:Password:ID=2,C=3}{ENTER}
      - DELAY types the characters 250 milliseconds apart
      - PICKCHARS uses field “PIN #” and selects 3 characters
      - PICKCHARS uses field “Password ” and selects 3 characters
      - ENTER completes the entry
    - Easier and more accurate than counting on fingers
    - See documentation for more examples

Database sharing

- Multiple machines can use a cloud file service such as TeamDrive or Dropbox to mirror a database file between the machines
  - It would be unwise to use the shared copy directly in case more than one machine updates the database
- KeePass synchronises two database files using “triggers”
  - Each machine has a local copy of the database. This synchronises to a mirrored cloud copy.
  - See <Sharing> and <Triggers for sharing> pages

KeePass Replication

- Replication via cloud storage



First Trigger

TAB = Properties
- Name = **Sync Demo to to Master when Local Database is opened**
- Name = Enabled = Ticked
- Name =Initially On = ticked

TAB = Events
- Add
  - Opened Database File (select from pull-down list)
    - File/URL – Comparison → Equals
    - File/URL – Filter → [full path to local file]
      [e.g. C:\Users\W10tst\Documents\KeePass\Demo (Local).kdbx]

TAB = Conditions
- Add
  - File Exists (select from pull-down list)
    - File/URL → [Full path to local database file]
      [e.g. C:\Users\W10tst\Documents\KeePass\Demo (Local).kdbx]

- Add
  - File Exists (select from pull-down list)
    - File/URL → [Full path to cloud database file]
      [e.g. C:\Users\W10tst\Documents\Spaces\Demo\KeyPass Demo\DemoDatabase (Master).kdbx]

TAB = Actions
- Add
  - Change trigger on/off state
    - Trigger name → [leave blank]
    - New State → Off
- Add
  - Change trigger on/off state (select from pull-down list)
    - Trigger name → **Sync Demo to to Master on Save/Close**
    - New State → Off (this is the default state)
- Add
  - Synchronize active database with File/URL(select from pull-down list)
    - File/URL → [Full path to local database file]
      [e.g. C:\Users\W10tst\Documents\KeePass\Demo (Local).kdbx]
- Add
  - Change trigger on/off state
    - Trigger name → [leave blank]
    - New State → On

Second Trigger

TAB = Properties
- Name = Sync Demo to to Master on Save/Close
- Name = Enabled = Ticked
- Name =Initially On = ticked

TAB = Events
- Add
  - Saving Database File (select from pull-down list)
    - File/URL – Comparison → Equals
    - File/URL – Filter → [full path to local file]
      [e.g. C:\Users\W10tst\Documents\KeePass\Demo (Local).kdbx]

TAB = Conditions
- Add
  - File Exists (select from pull-down list)
    - File/URL → [Full path to local database file]
      [e.g. C:\Users\W10tst\Documents\KeePass\Demo (Local).kdbx]
- Add
  - File Exists (select from pull-down list)
    - File/URL → [Full path to cloud database file]
      [e.g. C:\Users\W10tst\Documents\Spaces\Demo\KeyPass Demo\DemoDatabase (Master).kdbx]

TAB = Actions
- Add
  - Change trigger on/off state (select from pull-down list)
    - Trigger name → [leave blank]
    - New State → Off (this is the default state)
- Add
  - Synchronize active database with File/URL(select from pull-down list)
    - File/URL → [Full path to local database file]
      [e.g. C:\Users\W10tst\Documents\Spaces\Demo\KeyPass Demo\DemoDatabase (Master).kdbx]
- Add
  - Change trigger on/off state
    - Trigger name → [leave blank]
    - New State → On

Plugins

- KeePass has an internal architecture that supports <Plugins> that extend its functionality
- Many are available
- I use
  - KPEnhancedEntryView – Assists is viewing and updating custom fields
  - KPFieldsAdminConsole - Assists in maintaining custom fields
  - SourceForgeUpdateChecker – Assists in monitoring plugins for version cnages

Recommended Options (1)

- Setting “Rounds”
  - Keypass will take your “composite key” (e.g. password) and scramble it multiple times to generate the actual key used to encrypt/decrypt the database. The default is 6000 which is too low.
  - File → Database Settings → Security tab
  - Click “One Second Delay” to make the password computation take 1 second. In my test machine this gives a value of 3309056!
  - Use with care if sharing database with slower computers – it could take a long time to open

Recommended Options (2)

- Secure Desktop
  - KeePass supports a “Secure Desktop” which minimises the risk of a Key-logger intercepting your keystrokes while entering the password, Disabled by default.
  - Enable through Menu →Tools →Options
    - Select checkbox “Enter master key on secure desktop”

Recommended Options (3)

- Lock Database after inactivity
  - It is more secure to automatically lock the database if it has not been used.
  - Enable through Menu →Tools →Options
    - Select checkbox “Lock workspace after KeePass inactivity …”
    - Set the value if 300 seconds is not appropriate
    - I would also consider locking the computer when it is about to be suspended, and when locking the computer or switching users
    - Note that setting these options will mean you will need to enter your KeePass password more frequently!

Vital last words

- Backup your database!
  - and your key file if you use one
- Remember your master password!
  - You can never recover any passwords if you forget your password.
    - **There is no back door!**
- Do NOT use the Windows Account option
  - If your machine crashes you have lost your password database **including all backups**.
  - You cannot easily recreate your user account
    - One using the same name is not good enough