

PasswordPump II

User's Guide

Daniel Murphy, January 13, 2020

Contents

Initial Setup	2
Troubleshooting the Password Pump II	3
Uploading the Latest Firmware to the PasswordPump II	5
Features	5
Datasheets	6
Fixed Cost	7
Connections	7
RGB Colors and Meanings	9
Menu Navigation	10
Error Codes	12
Operation	13
Adding Credentials	14
Sending Credentials	16
Editing Credentials	16
Deleting Credentials	17
Generating a Password	17
Logging Out	18
Toggling Keyboard Entry	18
Showing/Hiding Passwords	18
Backing Up to EEprom	18
Back Up to a File	19
Restore a Backup from EEprom	19
Performing a Factory Reset	19

Initial Setup

When you first plug the PasswordPump II into a USB port you should see the following:

```
PasswordPump
Jan 12 2020
©2019 Dan Murphy
```

...and then

```
Main
Master Password
```

At this point you want to decide on a master password. A master password should be something that you can enter reasonably quickly using the rotary encoder, so if you're going to use a word think of one that's made up of characters from the beginning of the alphabet. For example; *cabbages* or *Abacus*. There are many other examples. You want a word or a combination of words and numbers that are not tedious to enter via the encoder. So I typically select a word that I can enter quickly followed by a four digit number. Of course you can enter anything you like, as long as it doesn't exceed 16 characters. It is possible to change the master password once you've entered it. If you want to change it and you haven't entered any credentials that you don't want to re-enter, then simply choose Factory Reset from the main menu. If you want to preserve all entered credentials, navigate to *Settings* and then to *Change Master Psswrd*.

Ok, so if you've thought of a master password you want to use. To start the process <ShortClick> the rotary encoder (press it down without holding it down for more than 0.5 seconds). Then use the rotary encoder to scroll to the first letter you want and <ShortClick> again. Continue entering characters in this fashion until they are all entered, then <LongClick> (hold down the rotary encoder for more than 0.5 seconds), and you'll see the following:

```
Main
Find Favorite
0 accounts
```

Remember your master password. If you forget it you'll lose access to all of the data you've entered, and short of breaking AES-256 somehow, you're not getting them back (unless you have exercised the feature that allows you to export all of your credentials to a file, which you should also encrypt).

You may also notice that when you first plug in the PasswordPump II that your operating system looks for drivers to install for the device. On Windows 7 and 10 I've had mixed experiences.

Sometimes everything works fine without having to take additional steps, and sometimes I have to manually install drivers supplied by AdaFruit. I've included those drivers in the repository for the PasswordPump II, here: https://github.com/seawarrior181/PasswordPump_II. Download and run `adafruit_drivers_2.4.0.0.exe` if necessary.

Now you're ready to start entering credentials. The easiest and best way to do that is via PasswordPumpGUI (a.k.a. `PassPumpGUI_v0_7.py`). It's a python program that serves up a user interface that you use to maintain credentials (account names, user names, passwords, previous password, and URL). To do that you need to use the rotary encoder to scroll down to *Edit with Computer* and <ShortClick>. Then you need to run `PasswordPumpGUI.py` on your computer and via it, open the correct port and start adding new sets of credentials!

Navigating through the menu on the PasswordPump II is explained on 5volts.org in the article for the PasswordPump (version 1.0). These instructions will eventually be updated to cover the PasswordPump II, but at this time they are the best reference for how to navigate the menus. Note that the menus for the PasswordPump v1.0 and the PasswordPump II are not the same. There are a lot more features available in the PasswordPump II, and there is also plenty of room for expansion in the future.

Troubleshooting the Password Pump II

- 1) *When I run `PasswordPumpGUI.py`, select the correct port and click Open, I see the following error message:*

```
C:\Users\someusername\Desktop>c:\python3\python
c:\PathToPasswordPumpGUI\PasswordPumpGUI.py
COM69: Adafruit ItsyBitsy M4 Express Arduino (802B:00) (COM69)
Connecting to arduino on COM69... done.
None
Exception encountered reading return value from pyReadHead; 'NoneType' object is
  not subscriptable
None
TypeError encountered in clickedOpen(); 'NoneType' object is not subscriptable
Opened port
```

This happens when you neglect to enter 'Edit with Computer' mode on the PasswordPumpII device before opening the port. If you have entered 'Edit with Computer' mode on the device and you're still seeing this error message, try power cycling the PasswordPump II, restarting the `PasswordPumpGUI.py` program, and trying again. In the extreme situation it's necessary to restart the computer to fix issues with the port in order to resolve this problem.

- 2) *When I select File->Import from PasswordPump from PasswordPumpGUI.py, navigate to and select a file, some sets of credentials import but eventually I see the following error message and the GUI freezes:*

```
Error encountered reading file in ImportFilePasswordPump; 'NoneType' object is not subscriptable
```

Click on the Exit button. If the UI remains frozen, click on the [x] close icon in the top right hand side of the window (under Windows). On the PasswordPump, long click the rotary encoder. If that doesn't return control, click on the reset button. Login to the device and re-select 'Edit with Computer'. Make sure that, in the export file, none fields contain a | (pipe) or a ~ (tilde). Make sure that none of the URLs end in / (forward slash). Launch PasswordPumpGUI.py and, once you select and open the correct port, re-try the import operation.

- 3) *When I enter an account name, username, password, or any other field that contains a ~ (tilde) or a | (pipe), that character is changed to a /1.*

Tildes and pipes are not supported in any of the fields. You'll need to eliminate them from your account name, username, password or other fields. This is an open defect in the tool.

- 4) *I'm using a Mac, Linux, or some other operating system other than Windows 7 or Windows 10, and things don't seem to be working correctly.*

Congratulations, you are the first person to use the product on your platform. Kindly let the PasswordPump II developer (dan-murphy@comcast.net) know about your issue(s) so that we can work on a solution. Your help is greatly appreciated. Alternatively use the forums at 5volts.org to solicit help.

- 5) *When navigating between accounts via the PasswordPumpGUI program the fields get out of synch; for example the account name appears on the Username text box, or fields are otherwise out of sync.*

The most likely cause of this problem is a | (pipe) character embedded in the account name, username, password, old password, or URL fields. To find the offending field edit

the fields of the offending credentials set via the rotary encoder on the PasswordPump II device. To identify the offending account, use the PasswordPumpGUI. Navigate between accounts, and when the alignment of fields looks wrong, take note of the previous account visited. The problem is most likely in one of the fields of the previously visited account. You can open up Notepad (if you're running Windows), and paste the username, password, account name, URL and old password into Notepad. Note if any of the fields have an embedded | (pipe) character.

Uploading the Latest Firmware to the PasswordPump II

To burn the latest version of the firmware, first download PasswordPumpM4_01.ino.bin from https://github.com/seawarrior181/PasswordPump_II and save it to C:\temp. Find where the **bossac** utility is installed on your system and modify the path below as per its location. Identify the port to which the ItsyBitsy/PasswordPump is connected and substitute the correct port number in the command below. Double click on the reset button at the bottom of the PasswordPump. The RGB LED will slowly dim and brighten in blue over and over again. From a command window (<Alt><Esc>cmd<Return>) execute a command similar to the following:

```
C:\Users\username\AppData\Local\Arduino15\packages\arduino\tools\bossac\1.8.0-48-gb176
eee\bossac -i -d --port=COM52 -U -i --offset=0x4000 -w -v
C:\Temp>PasswordPumpM4_01.ino.bin -R
```

At this time it's also important to download the latest version of the PasswordPumpGUI; which is presently here:

https://github.com/seawarrior181/PasswordPump_II/blob/master/PassPumpGUI_v0_7.py.

At a point in the near future the version numbers will be synchronized to make it more obvious that a particular version of the firmware only works with a particular version of the PasswordPumpGUI.

Features

- Authenticate with 16 character master password
- Search for accounts
- Send user name and password as if typed in keyboard
- Add account name, user name, password (generated or not), url, old password

- Edit existing user name, password, URL, style (inter-username/password character, <Return> or <Tab>)
- Delete account
- Generate password
- Store old password
- Data entry via rotary encoder or keyboard and serial monitor, or via client Python program running in Windows.
- Accounts added in alphabetical order
- Store up to 254 sets of credentials
- Backup all accounts to a second encrypted external EEPROM
- Logout / de-authenticate via menu
- Factory reset via menu (when authenticated)
- Configurable password display on or off
- Configurable failed login count factory reset (3, 5, 10, 25)
- Configurable automatic logout after count of minutes (30, 60, 90, 120, 240, 1, Never)
- Configurable RGB LED intensity (high, medium, low, off)
- All passwords (except master password) are encrypted w/ AES-256; master password is hashed w/ SHA-256.
- Change master password
- Export/Import to/from PasswordPump CSV format (dumps output to an editor)
- Import KeePass exported CSV file
- Import passwords from Chrome
- Associate credentials with groups for better organization; search by group (Favorites, Work, Personal, Home, School, Financial, Mail, Custom)
- Decoy password feature that automatically factory resets the device if entered (e.g. while the user is under duress)
- Pre-auto-logout indicator via flashing RGB LED.

Datasheets

AdaFruit ItsyBitsy (32-bit ARM®, SAMD51 Cortex®-M4F MCU)

Data Sheet: <http://ww1.microchip.com/downloads/en/DeviceDoc/60001507E.pdf>

MICROCHIP - 25LC512-I/P - 512K SPI™ Bus Serial EEPROM DIP8, one primary one backup.

Data Sheet: <http://ww1.microchip.com/downloads/en/DeviceDoc/20005715A.pdf>

SSD1306 I2C LED display 128x32 pixels.

Data Sheet: <https://cdn-shop.adafruit.com/datasheets/SSD1306.pdf>

<https://www.vishay.com/docs/37894/oled128o032dlpp3n00000.pdf>

Fixed Cost

1 AdaFruit ItsyBitsy (32-bit ARM®, SAMD51 Cortex®-M4F MCU)	\$14.95
2 MICROCHIP - 25LC512-I/P - 512K SPI™ Bus Serial EEPROM DIP8	3.80
1 SSD1306 I2C LED display 128x32 pixels.	2.23
1 Custom PCB	1.50
1 micro USB to USB cable 100cm	0.69
1 Rotary Encoder	0.46
1 plastic knob for rotary encoder	0.11
2 IC DIP Sockets, 8 pins each	0.10
Solder	0.10
1 RGB LED diffused 5mm	0.03
3 220ohm resistors	0.01
2 4.7kohm resistors	0.01

Total Parts	\$23.99
	=====
+ Labor for assembly, packaging & shipping	

Connections

ItsyBitsy M0/M4

<u>Num</u>	<u>Name</u>	<u>Connect To / Notes</u>
1	RS	reset button
2	3V	25LC256 Prim Pin 3 & 25LC256 Secondary Pin 3
3	AREF	
4	VHI	
5	A0	
6	A1	
7	A2	
8	A3	
9	A4	220 Ohm resistor->RGB LED Pin 3
10	A5	
11	SCK	25LC256 Prim Pin 6 & 25LC256 Secondary Pin 6
12	MO	25LC256 Prim Pin 5 & 25LC256 Secondary Pin 5
13	MI	25LC256 Prim Pin 2 & 25LC256 Secondary Pin 2
14	2	

15	En	
16	swdio	
17	swclk	
18	3	
19	4	
20	RX	
21	TX	
22	SDA	SSD1306 SDA, 4.7k Ohm resistor->ItsyBitsy Pin 31
23	SCL	SSD1306 SCL, 4.7k Ohm resistor->ItsyBitsy Pin 31
24	5! (VHI Out)	220 Ohm resistor->RGB LED Pin 4
25	7	Rotary Encoder Pin 3
26	9	Rotary Encoder Pin 1
27	10	25LC256 Secondary Pin 1 Chip Select
28	11	25LC256 Primary Pin 1 Chip Select
29	12	Rotary Encoder Pin 4
30	13	220 Ohm resistor->RGB LED Pin 1
31	USB	SSD1306 VCC
32	G	RGB LED Pin 2, 25LC256 Prim & Secon Pin 4, SSD1306 Pin 1, Rotary Encoder Pins 2 & 5
33	BAT	

2 25LC512 (External EEprom)

Tested Part: MICROCHIP - 25LC512-I/P - 512K SPI™ Bus Serial EEPROM DIP8

25LC512 Primary

<u>Num</u>	<u>Name</u>	<u>ConnectTo</u>	<u>Note</u>
1	CS	pin 28 ItsyBitsy	Chip Select Input
2	SO	pin 13 ItsyBitsy	MISO - Serial Data Output
3	WP	pin 2 ItsyBitsy	Write Protect
4	Vss	pin 2 ItsyBitsy	Ground
5	SI	pin 12 ItsyBitsy	MOSI - Serial Data Input
6	SCK	pin 11 ItsyBitsy	SCLK - Serial Clock Input
7	HOLD	pin 2 ItsyBitsy	Hold Input
8	Vcc	pin 2 ItsyBitsy	Supply Voltage

25LC512 Secondary

<u>Num</u>	<u>Name</u>	<u>ConnectTo</u>	<u>Note</u>
1	CS	pin 27 ItsyBitsy	Chip Select Input
2	SO	pin 13 ItsyBitsy	MISO - Serial Data Output
3	WP	pin 2 ItsyBitsy	Write Protect
4	Vss	pin 2 ItsyBitsy	Ground
5	SI	pin 12 ItsyBitsy	MOSI - Serial Data Input
6	SCK	pin 11 ItsyBitsy	SCLK - Serial Clock Input

7	HOLD	pin 2 ItsyBitsy	Hold Input
8	Vcc	pin 2 ItsyBitsy	Supply Voltage

Rotary Encoder

1 2 3
4 5

<u>Num</u>	<u>Name</u>
1	ItsyBitsy Pin 26
2	ItsyBitsy Pin 32
3	ItsyBitsy Pin 25
4	ItsyBitsy Pin 29
5	ItsyBitsy Pin 32

SSD13306

GND VCC SCL SDA
1 2 3 4

<u>Num</u>	<u>Name</u>	<u>ConnectTo</u>
1	GND	ItsyBitsy Pin 32
2	VCC	ItsyBitsy Pin 31
3	SCL	ItsyBitsy Pin 23
4	SDA	ItsyBitsy Pin 22

RGB LED

<u>Num</u>	<u>Name</u>	<u>ConnectTo</u>
1	Red	220 Ohm resistor->ItsyBitsy Pin 30
2	Grnd	ItsyBitsy Pin 32
3	Green	220 Ohm resistor->ItsyBitsy Pin 9
4	Blue	220 Ohm resistor->ItsyBitsy Pin 24

RGB Colors and Meanings

<u>Color</u>	<u>Meaning</u>
Green	Logged in
Orange	Backing up EEprom memory
Alternating Blue and Red	Initializing EEprom or auto logout pending
Purple	Sending creds, backing up to EEprom, editing with computer.
Red	Error backing up or initializing EEprom, failed login attempt(s).

Yellow
Blue

Error backing up or initializing EEprom
Not logged in including failed login attempt

Menu Navigation

You move through the menu items by turning the rotary encoder, clockwise to move down the list and counter clockwise to move up. Account names are stored in alphabetical order. To select an item you click down on the rotary encoder (short click). To backup you hold the rotary encoder down for more than a half second (long click).

- Master Password
- Find Favorite
- Find All Accounts
 - [scroll through accounts list]
 - Send Password <RET>
 - Send User & Pass
 - Send URL
 - Send User Name
 - Send Pass (no <RET>)
 - Send Account
- Edit Credentials
 - Edit Account Name
 - Edit User Name
 - Edit Password
 - Edit URL
- Indicate Style
- Assign Groups
 - Favorites
 - Work
 - Personal
 - Home
 - School
 - Financial
 - Mail
 - Custom
- GeneratePassword
- Save to Old Password
- Delete Credentials [confirm]
- Send Old Password

Find By Group

Favorites

[same as under Find All Accounts]

Work

[same as under Find All Accounts]

Personal

[same as under Find All Accounts]

Home

[same as under Find All Accounts]

School

[same as under Find All Accounts]

Financial

[same as under Find All Accounts]

Mail

[same as under Find All Accounts]

Custom

[same as under Find All Accounts]

Add Account

Account Name

Edit User Name

Edit Password

Indicate Style

GeneratePasswrd

Logout

Backup/Restore/Imprt

Backup EEprom [confirm]

Restore EEprn Backup [confirm]

Backup to .CSV File

Import PasswordPump

Import KeePass

Settings

Keyboard ON/OFF

Show Passwrd ON/OFF

Decoy Password ON/OFF

RGB LED Intensity

High

Medium

Low

Off

Timeout Minutes

30

60

90

120
240
Never
1
Login Attempts
3
5
10
25
Change Master Password
Factory Reset [confirm]

Error Codes

000 - SSD1306 allocation failed (only visible via serial)
001 - Error navigating Off On menu
002 - Error navigating main menu
003 - Error navigating edit credentials menu
004 - Error navigating send credentials menu
005 - Error navigating settings menu
006 - Error showing credential values
007 - Unrecognized event
008 - Invalid state when showing Off On menu
009 - Invalid login attempt maximum
010 - Out of space
011 - Corruption found
012 - Out of space during import
013 - Failed to open file for import
014 - Failed to mount FAT file system during import
015 - Failed to initialize flash during import
016 - Invalid RGB LED Intensity position
017 - Invalid maximum login attempt count
018 - Invalid logout timeout value
019 - Invalid keyboard, show password or decoy password value
020 - Account name keeps encrypting to 255 in first char during import
021 - User name is too long on import
022 - Password is too long on import
023 - Web site is too long on import
024 - Account name is too long on import
025 - Invalid group specified

- 026 - Invalid search group specified
 - 027 - Invalid group menu item specified
 - 028 - Invalid state during event single click
 - 029 - Invalid state encountered during rotate counter clockwise event
 - 030 - Invalid state encountered during rotate clockwise event
 - 031 - Empty credentials found in linked list
 - 032 - Corrupt linked list
 - 033 - Corrupt linked list in FindAccountPos.
 - 034 - Failed to initialize flash during PasswordPump CSV file import
 - 035 - Group length is greater than one
 - 036 - Too many fields found in PasswordPump CVS file during import
 - 037 - Failed to open PasswordPump CVS file for import
 - 038 - Invalid position in file menu
 - 039 - Encrypted account name starts with 255, fixing...
 - 040 - Invalid position when returning to a find by group menu
 - 041 - Corrupt link list encountered while counting accounts
-

Operation (these are the operating instructions for the PasswordPump v1.0, they will eventually be updated)

To turn the device on you simply plug it into a USB port/receptacle using a micro USB Micro-B plug to USB-A plug cable, the same cable that you'd use to charge an Android phone. The first time you plug it in a driver might need to be installed. The driver is available for download in the source code repository referenced below in the Source Code section. If I shipped the device to you it arrives already flashed with the program and the lock bits are set. See the data sheet, section 28.1, for more information about setting the lock bits. Since this is an open source project it doesn't really matter anyhow.

Setting the lock bits serves to better protect the hashed master password and the source code.

The first time you power the device on you'll see :

Master Password

March 11 2019 (or the date of the most recent compile)

At this point you'll want to enter your master password. Try to select a password that can be more quickly entered into the device. It should be a combination of upper and lower case, with numbers and maybe a symbol or two. I like to pick a password that can be typed almost entirely

with my left hand, I find they are easier to input via the rotary encoder. You should select a strong password; a combination of letters, upper and lower case, numbers, and special characters, between 7 and 14 characters long. To enter a character turn the rotary encoder until the character appears and then press the rotary encoder down (short click) to select the character. There's presently no way to back up if you make a mistake so be careful. Once the entire master password has been entered long click the device (click down the rotary encoder for more than 1/2 a second). You've just entered the master password and now you're ready to enter a set of credentials.

You move through the menu items by turning the rotary encoder, clockwise to move down the list and counter clockwise to move up. Account names are stored in alphabetical order. To select an item you click down on the rotary encoder (short click). To backup you hold the rotary encoder down for more than a half second (long click).

Note: The following instructions describe the easiest way to enter credentials if you don't have access to the PasswordPumpGUI or if it's not working correctly. The easiest way to enter credentials is via the PasswordPumpGUI, and it's fairly self-explanatory, so use that method if possible.

Adding Credentials

To add a set of credentials via the keyboard you need to open a serial terminal. The one that works best for me is the Arduino serial terminal. So if you open the Arduino IDE go to Tools->Ports and select the *Arduino/Genuino Micro* port. Then select Tools->Serial Monitor (or Ctl+Shift+M). Next, on your PasswordPump navigate down to Keyboard OFF and change it to Keyboard ON with a short click. Navigate back up to Add Account and short click. You'll see:

Account Name

Add Account

Short click, then switch back to the Arduino Serial Terminal and enter the account name, followed by the return key. Then long click on the Password Pump. You should now see:

Edit Username

[the account name you entered]

Short click again, switch back to the Arduino Serial Terminal and enter the username, followed by the return key. Then long click on the Password Pump. You should now see:

Edit Password

[the account name you entered]

Short click again, switch back to the Arduino Serial Terminal and enter the password, followed by the return key. Then long click on the Password Pump. You should now see:

Indicate Style

[the account name you entered]

Short click again and use the rotary encoder to specify either 0 or 1. Specify 0 if, while supplying username and password, the Password Pump should send a carriage return after sending the username and before sending the password. Specify 1 if, while supplying username and password, the Password Pump should send a tab after sending the username and before sending the password. Then long click on the Password Pump. You should now see:

Account Name

[the account name you entered]

Long click again and you'll see:

Find Account

[the account name you entered]

You've finished entering the credentials.

Note that you can also enter credentials using just the rotary encoder. Keyboard can be ON or OFF, it doesn't matter. Simply enter the credentials using the rotary encoder in a fashion similar to how you entered the master password.

Sending Credentials

Navigate to Find Account and short click. Use the rotary encoder to scroll through the list of credentials you've entered. When you've found the account name associated with the credentials you want to send to your computer, place the input focus in the username text box in the window prompting you for credentials on your computer. On the Password Pump you should see:

Send User & Pass
[the account name you selected]

Short click to send the username, a carriage return or a tab character (depending on the style setting), and then the password. If you selected the correct style you should now be logged in to your account / application.

If you only want to send the password to the computer, followed by a carriage return, scroll down once using the rotary encoder until you see:

Send Password <RET>
[the account name you entered]

And short click to send the password and the carriage return character.

Similarly you can send just the username or just the account name.

Editing Credentials

To edit a set of existing credentials first decide if you're going to edit the credentials via the keyboard or just the rotary encoder. If you're going to edit the credentials via the keyboard follow the instructions in *Toggling Keyboard Entry*. Then use *Find Account* to navigate to the account you want to edit and short click. Then scroll down to *Edit Creds* and short click. Then

scroll to the attribute you want to edit; *Account Name*, *Edit Username*, *Edit Password*, or *Indicate Style*. Now short click. Use the keyboard to re-enter the attribute in the fashion described in *Adding Credentials*, or just use the rotary encoder to re-enter the attribute. Then long click to save the change. If you are generating a new password for the account then follow the instructions in *Generating a Password*.

Deleting Credentials

Make sure you have a current EEprom backup. Navigate to *Find Account* and short click. Use the rotary encoder to select the account that you want to delete, and short click. Using the rotary encoder scroll down to *Delete Acct* and short click. Confirm your desire to delete the account by selecting Y with the rotary encoder and short clicking. The account is gone now and it's wiped from the primary EEprom chip. It isn't wiped from the backup EEprom yet, so if you accidentally delete an account, and you have a recent backup, you can restore the backup and the account will reappear. Navigate to *Find Account* and verify that your account is deleted. If you're not able to scroll through all of your accounts, a intermittently occurring defect has occurred and the linked list that manages the display of all of the accounts is corrupted. Restore the latest backup from EEprom. If you backup the EEprom immediately after deleting the account it is also wiped from the secondary EEprom.

Generating a Password

Read through all of these instructions before attempting to change your password to a new generated password. The most powerful feature of the PasswordPump is it's ability to generate random 31 character passwords and remember them. These passwords are extremely difficult to guess and are not as vulnerable to brute force attempts to break into an account. Before performing this operation you should be sure that you have a current backup of all your credentials. To generate a password for an account simply find the account via *Find Account* and select the credentials by short clicking on the account name. In your application on your computer navigate to the change password feature and place input focus in the Old Password text box. On the PasswordPump navigate to *Send Password* (NOT *Send Password <RET>*) and short click. In your application on your computer place input focus in the new password text box by hitting the <TAB> key. In the PasswordPump scroll down to *Edit Creds* and short click, then scroll down to *Gen Password* and short click. This changes the password to a randomly generated series of 31 characters. Now long click once, navigate to *Send Password* (NOT

Send Password <RET>) and short click. If you need to confirm the new password then place input focus on that text box in the application on your computer and short click again. Confirm your password change by hitting the return key or otherwise clicking on the appropriate button. You now have a random 31 character password on the account, and the only place where that password exists is on the encrypted EEPROM chip on your PasswordPump. At this point it's a good idea to *Backup to EEPROM* and *Backup to a File*, and to be sure that you can somehow recover from a lost password on that account. Warning: If the attempt to change your password fails because the old password is not accepted be aware that you have just overwritten the old password with your new generated password. To restore the old password you'll need to either *Restore a Backup from EEPROM* and try again, or go to the encrypted backup file on your thumb drive to get the current password for the account, or recover the password from the account using whatever mechanism is available to you via the application or web site. Think ahead and be careful so that you don't lock yourself out of your account!

Logging Out

When you want to log out of the device navigate to *Logout* using the rotary encoder and short click. The RGB led changes from green to blue. You're now logged out and must enter the master password again in order to use the device. If you're walking away from your computer to get coffee it's good practice to lock your computer and logout of the PasswordPump.

Toggling Keyboard Entry

Navigate to *Keyboard ON/OFF*. Short click to toggle the setting. When the keyboard is on you may enter credentials via the keyboard using the process described in *Adding Credentials*. Keep the keyboard set to OFF when you're not entering credentials. This setting is not saved when the device powers off and the default is *Keyboard OFF*.

Showing/Hiding Passwords

Using the rotary encoder navigate to *Show Psswrd ON/OFF*. Short click to toggle the setting. This setting is saved when you log out and power down the device.

Backing Up to EEPROM

On the Password Pump navigate to *Backup EEPROM* using the rotary encoder. Short click, then confirm that you want to backup from the primary EEPROM to the secondary EEPROM by

selecting *Y* with the rotary encoder and short clicking. The RGB will be yellow while the backup is taking place, and then change back to green.

Back Up to a File

On the PasswordPump navigate to *Backup to File* using the rotary encoder. On your computer open a text editor (one without an autocomplete feature), notepad.exe works best, and place input focus inside the text editor. Personally I use UltraEdit because it has built in encryption. Then short click on *Backup to File*. The contents of the primary EEprom chip (all of the credentials stored in the PasswordPump) are dumped into the text editor. The RGB led turns purple, then to green when the operation is complete. It's best to encrypt this file by zipping it up with a password using WinZip or similar, and storing it on a thumb drive that you can, in turn, store in a safe or safe deposit box. Delete the original file from your computer and empty the trash. Keep this file up to date by periodically executing this operation. I carry the encrypted file with me on a thumb drive that is securely attached to my key ring, and I keep a backup of that file elsewhere.

Restore a Backup from EEprom

If you decide that you want to restore the EEprom backup (or, in other words, have the contents of the secondary, backup EEprom overwrite the contents of the primary EEprom), then navigate to *Restore Backup* on the PasswordPump. Short click and confirm the operation by selecting *Y* with the rotary encoder and short clicking. The RGB led will turn yellow until the operation is complete, then it changes back to green.

Performing a Factory Reset

You want to wipe out all of the encrypted credentials on the primary EEprom and factory reset the device. On the PasswordPump navigate all the way down to *Reset* using the rotary encoder. Short click. Confirm that you want to factory reset the device and clear all of the credentials and the master password by selecting *Y* with the rotary encoder and short clicking. The RGB will flash blue and red slow and then fast while the device is factory resetting, then change to blue. At this point you can enter a new master password. Note that a Factory Reset doesn't wipe out the credentials stored on the backup EEprom. If you use the same master password you'll be able to restore the backup and see the credentials. If you want to wipe out the backup EEprom as well, select *Backup EEprom* after you've entered your new master

password, or swap the position of the primary and backup EEPROM chips and perform another factory reset.

Usage Notes, Suggestions & Disclaimers

- Do not make a habit out of unplugging the device from its micro-B USB port. Instead unplug the end of the cord that plugs directly into the computer (USB A), and leave the device plugged into the cord. This reduces the wear and tear on the device's micro USB port and will extend the life of the unit. I have seen similar micro-B USB ports fail.
- If you have many accounts, associate the accounts you use the most with the Favorites group. Of these favorite accounts, name the accounts you use the most with an _ (underscore) so that they will sort to the top of the favorites list. I use this technique to identify my MS Active Directory credentials, which I have to supply in many places. That account is named _Active Directory. After I login to the device I can short click three times and my _Active Directory password is typed into the computer via the PasswordPump.
- A master password should be something that you can enter reasonably quickly using the rotary encoder, so if you're going to use a word think of one that's made up of characters from the beginning of the alphabet. For example; *cabbages* or *Abacus*. There are many other examples. You want a word or a combination of words and numbers that are not tedious to enter via the encoder. So I typically select a word that I can enter quickly followed by a four digit number. Of course you can enter anything you like, as long as it doesn't exceed 16 characters. Even a four digit pin might be secure enough for you.
- Remember to *Backup to EEPROM* after changing attributes of existing credentials or after inserting new credentials. I usually confirm that I can navigate through all existing accounts forwards and backwards before executing a *Backup to EEPROM* operation.
- Immediately after performing a *Change Master Password* operation, confirm that you can navigate through all the accounts forwards and backwards, then perform a *Backup to EEPROM* operation. If for some reason your credentials look corrupted after a *Change Master Password* operation, *Restore EEPROM Backup* will restore your credentials to the device with the original master password.
- Before removing the EEPROM chip(s) from the device, power it off by unplugging it from your computer.
- Instead of executing a *Restore EEPROM Backup* operation you can swap the positions of the EEPROM chips instead.
- Maintain a third EEPROM backup and secure it in a safe place.
- Use the PasswordPumpGUI to create a PasswordPump formatted .csv file. Encrypt this file and/or store it on an encrypted thumb drive, and store the thumb drive in a safe or safe deposit box (perhaps alongside your EEPROM backup). If your PasswordPump's

data becomes corrupted you can perform a *Factory Reset* operation and then Import Password Pump file via the PasswordPumpGUI. If you are diligent about backing up your credentials in this manner you can use the PasswordPump as your system of record for all of your credentials.

- **Important:** It is also possible to create a .csv file by opening Windows Notepad.exe (or a similar editor on other operating systems), placing input focus in the editor's window, and selecting the *Backup to .CSV File* operation on the PasswordPump. It is extremely important to make sure that input focus remains inside the editor while this operation is underway, otherwise credential sets will be provided to whatever application takes the input focus, and this results in undefined behavior from the computer. I am considering the removal of this feature from the device because you can achieve the same result via the PasswordPumpGUI. If you find yourself executing this feature by accident and the input focus is not in a text editor, simply unplug the PasswordPump from the USB port.
- **Disclaimer:** The PasswordPump is not secure from keylogging attacks (https://en.wikipedia.org/wiki/Keystroke_logging). Keylogging attacks are capable of stealing passwords that are entered through your keyboard. All data sent to your computer with the PasswordPump enters the computer as if through a keyboard. Therefore you should remain diligent about protecting yourself from these kinds of attacks. See the countermeasures section of the Wikipedia link provided above.
- **Disclaimer:** The contents of the EEprom chips on the PasswordPump are encrypted with AES-256, and the master password is hashed with SHA-256. The unhashed master password serves as the encryption key (along with 16 bytes of salt). Nevertheless, if somebody with nefarious purposes obtains access to your PasswordPump it's best to assume that all of your credentials have been compromised. It is possible to move the encrypted contents of the EEprom to an operating system file by using a USB programmer (e.g. TL866II Plus). This would allow an attacker to circumvent the protections built into the device that prevent more than 3, 5, 10 or 25 failed login attempts before the credentials are wiped. I will consider removing this advice when the device's software has been subjected to a rigorous code review by encryption industry experts.
- EEprom chips can be moved to another PasswordPump device and will continue to function without modification. The hashed master password and salt are stored in the external EEprom chips.
- If the Old Password field is empty, it's automatically populated with the existing password when the Generate password button is clicked in the PasswordPumpGUI. If the field is *not* empty, clicking on the Generate password button will *not* move the existing password to the Old Password field, but it will overwrite the existing password with the generated password. If the Old Password field is populated and you want the existing password to move to the Old Password field after clicking the Generate button (which would be the typical use case), then blank out the Old Password *before* clicking on Generate. The Old Password field is intended to protect the user from the situation whereby a password change is being made, the Generate button is selected to generate a new password, but the application or website for which your changing the password

does not accept the newly generated password for any reason and you have therefore lost the currently active password. By use of the Old Password field, In this situation, you have not lost the currently active password, it is in the Old Password field.

- Use of the PasswordPumpGUI currently requires the installation of Python 3.8. At some point in the future an .exe will be created so that this requirement can be removed.
- *Import PasswordPump*, *Import KeePass*, and *Import Chrome* operations directly from the PasswordPump device are deprecated, these use cases can now be executed via PasswordPumpGUI.
- Source code is located here: https://github.com/seawarrior181/PasswordPump_II
- Send any issues and suggestions to dan-murphy@comcast.net.