Pa55ware

A simple, DIY hardware password manager

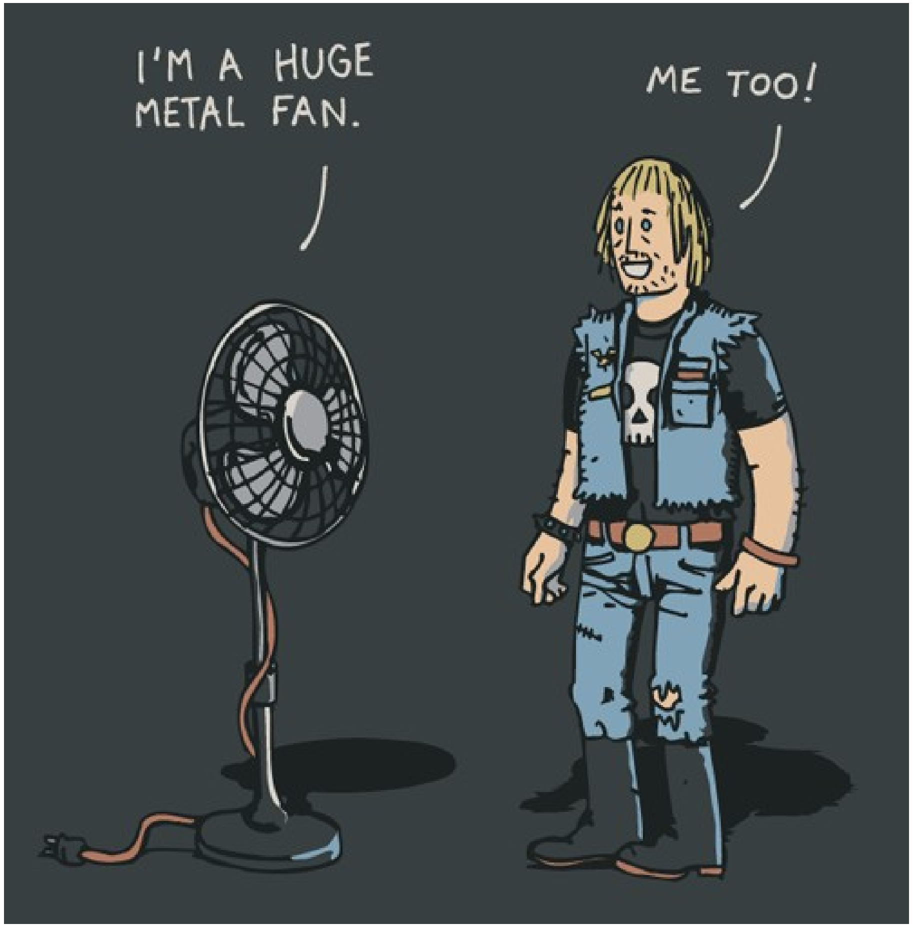
Passwordscon 2013, Bergen

Who are those guys ?

- Nicolas “Balda” Oberli
  - @Baldanos
- Security engineer
- CTF player
- Conference speaker
- Hacker / Mad scientist
- Beer brewer / drinker

Who are those guys ?

- Manoé “Sata” Zwahlen
- Security engineer
- CTF player
- Developer of Fireforce
- Black metal fan



Passwords suck

- Not cool, but they are used everywhere
- Managing passwords is hard
  - Lots of passwords to remember
  - We tend to reuse passwords or have a password scheme

Password managers

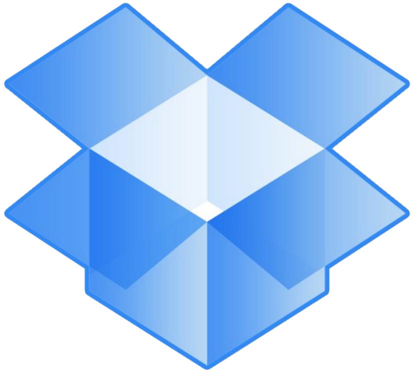
- Good thing
  - Secure !
  - You only need to remember one password to access all the others
- A lot of them exist

Password managers - cont

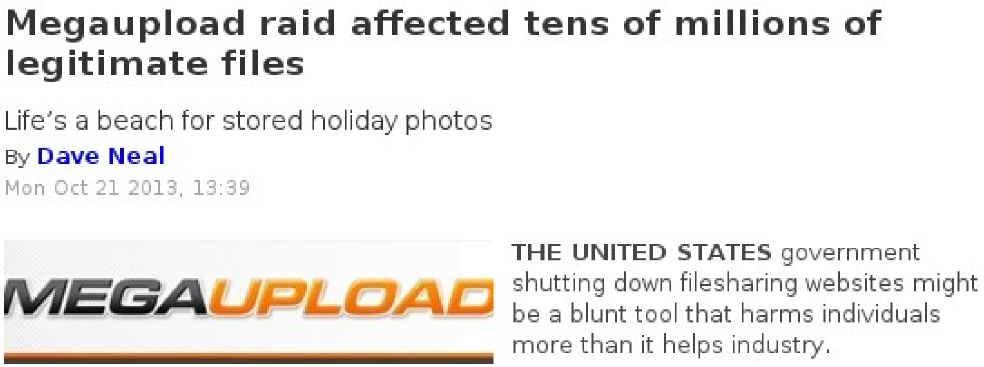
- They also suck !
  - If someone gets access to your database, you are at risk
    - keepass2john, passwordsafe cracker, ...
  - How do you use it while on travel ?
    - Many of them are available on a single platform
  - Do you really want to install the application on an unknown machine ?
    - Or type your master password on it ?

Password managers - Storage

- How do you backup your password database ?



Really ?



Megaupload raid affected tens of millions of legitimate files

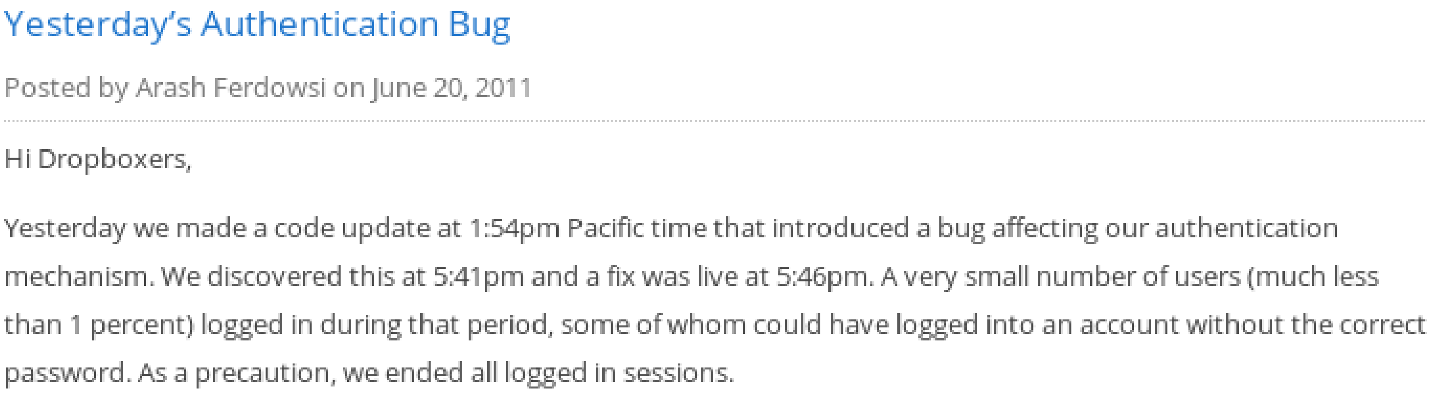
Life's a beach for stored holiday photos

By **Dave Neal**

Mon Oct 21 2013, 13:39

THE UNITED STATES government shutting down filesharing websites might be a blunt tool that harms individuals more than it helps industry.

http://www.theinquirer.net/inquirer/news/2301904/megaupload-raid-affected-tens-of-millions-of-legitimate-files



Yesterday's Authentication Bug

Posted by Arash Ferdowsi on June 20, 2011

Hi Dropboxers,

Yesterday we made a code update at 1:54pm Pacific time that introduced a bug affecting our authentication mechanism. We discovered this at 5:41pm and a fix was live at 5:46pm. A very small number of users (much less than 1 percent) logged in during that period, some of whom could have logged into an account without the correct password. As a precaution, we ended all logged in sessions.

https://blog.dropbox.com/2011/06/yesterdays-authentication-bug/

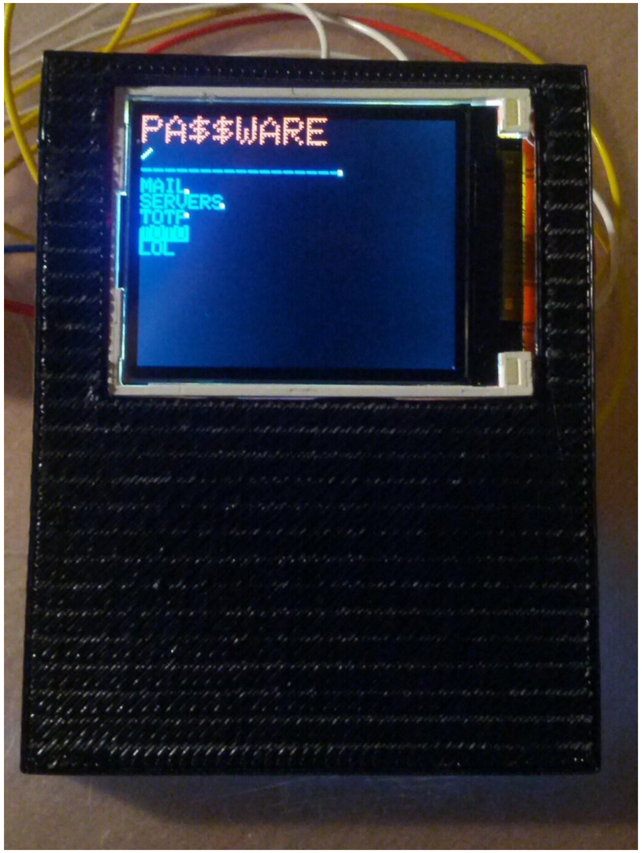
And of course....

What can we do ?

- Passwords are like keys to our online places
- Why don't we store and use them like real keys ?
  - You always have them on you
  - You may have a backup, but you (probably) know where they are
  - You wouldn't let anyone take care of them

Introducing Pa55ware

- Like a keyring, but for passwords
- Keep your passwords with you
- Use them when you want to



Why Pa55ware ?

- Manage **PA55**w0rd$ with hard**WARE**
  - With a (strong) Belgian accent, it means sieve
    - And also because passware is already used

http://commons.wikimedia.org/wiki/File:Sieve.jpg

Pa55ware - Features

- Easy to use
  - 4 touch buttons to navigate
  - A LCD screen to view your passwords
  - A client application is used to manage data stored on the device

Pa55ware - Features

- Safe to use
  - Everything is encrypted using AES
    - The passwords and data are stored on a SD card
    - The key is stored on the device, there is no way to retrieve it
  - A PIN code is used to unlock the device
    - Make it wrong too many times and the AES key is gone

Pa55ware - Features

- Practical to use
  - Pa55ware can handle your OTP
    - Currently only TOTP is implemented (Google auth)
  - It can type your passwords for you
    - Acts like a USB keyboard
    - Works on nearly every kind of device

Pa55ware - Features

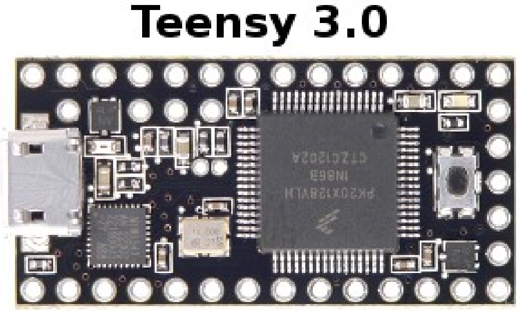
- Free to use
  - Everything is open source
    - GPLv2 licensed
    - Yes, even the case
  - It's easy to make one
    - You'll need a soldering iron and access to a 3D printer

Bill of Materials

Name	Where to find ?	Cost
Teensy 3.0	PJRC	$19
TFT LCD + SD card reader	ElecFreaks	$12
SD card	Amazon	$7
TOTAL		**$38**
3D printer access	??	??
Wire and solder	??	??

Pa55ware core

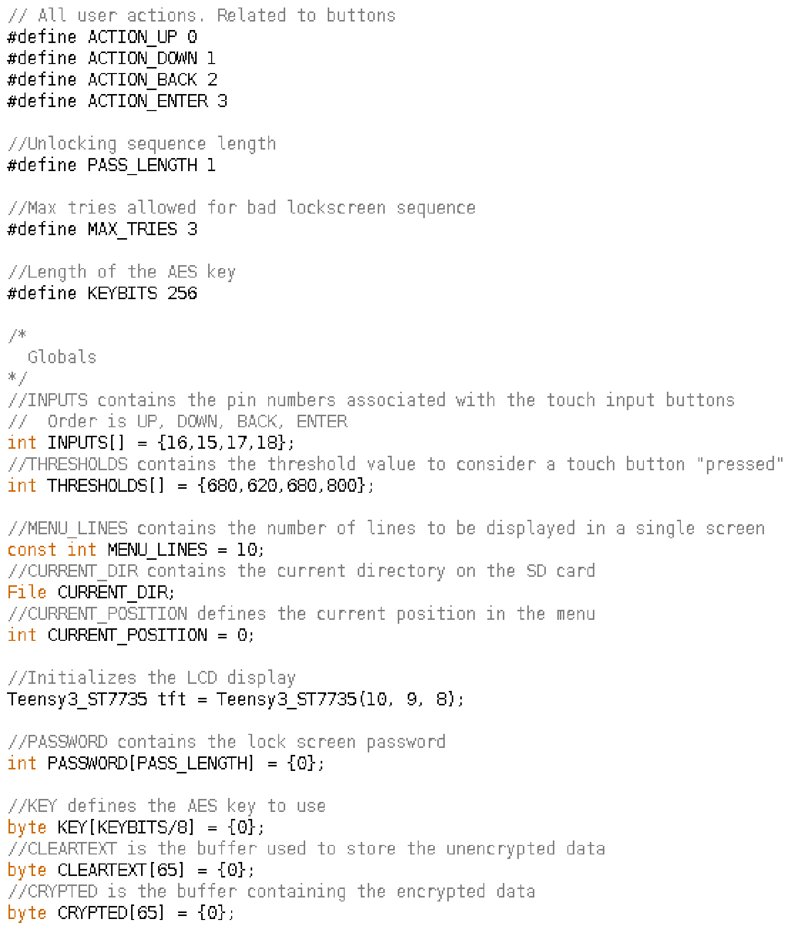
- The main component is a Teensy 3.0
  - ARM core
  - Many inputs/outputs
  - Capacitive (touch) inputs are available
  - Can be used with the Arduino IDE
  - Has an internal RTC
- It's just awesome !



http://www.pjrc.com/teensy/teensy3.png

Code

- Everything is written using the Arduino IDE
  - Easy to get into it
- Easily customisable
  - Edit the initial variables and you're good



```
// All user actions. Related to buttons
#define ACTION_UP 0
#define ACTION_DOWN 1
#define ACTION_BACK 2
#define ACTION_ENTER 3

//Unlocking sequence length
#define PASS_LENGTH 1

//Max tries allowed for bad lockscreen sequence
#define MAX_TRIES 3

//Length of the AES key
#define KEYBITS 256

/*
  Globals
*/
//INPUTS contains the pin numbers associated with the touch input buttons
//  Order is UP, DOWN, BACK, ENTER
int INPUTS[] = {16,15,17,18};
//THRESHOLDS contains the threshold value to consider a touch button "pressed"
int THRESHOLDS[] = {680,620,680,800};

//MENU_LINES contains the number of lines to be displayed in a single screen
const int MENU_LINES = 10;
//CURRENT_DIR contains the current directory on the SD card
File CURRENT_DIR;
//CURRENT_POSITION defines the current position in the menu
int CURRENT_POSITION = 0;

//Initializes the LCD display
Teensy3_ST7735 tft = Teensy3_ST7735(10, 9, 8);

//PASSWORD contains the lock screen password
int PASSWORD[PASS_LENGTH] = {0};

//KEY defines the AES key to use
byte KEY[KEYBITS/8] = {0};
//CLEARTEXT is the buffer used to store the unencrypted data
byte CLEARTEXT[65] = {0};
//CRYPTED is the buffer containing the encrypted data
byte CRYPTED[65] = {0};
```

SD card storage

- Uses a simple FAT filesystem
  - May be used to create backups
- Each account is stored in a separate binary file
- Drawback : Filenames are limited in length

File format

[File header]	\x42
[File type]	\x01 : Username/password file
	\x02 : OTP seed file
[section1]	
[ID]	\x01 : Username
	\x02 : Password
[length]	variable
[data]	AES encrypted data
[section2]	
...	

Sensitive data

- The AES key is the most important thing to protect
  - It is loaded from the internal EEPROM once the device is unlocked
  - AES key is cleared from memory as soon as the device is locked again

Memory management

- Every cleartext data is cleared as soon as it is not used anymore
  - This prevents the RAM from being read externally
- Efforts have been made to make it efficient and bug free

Communication

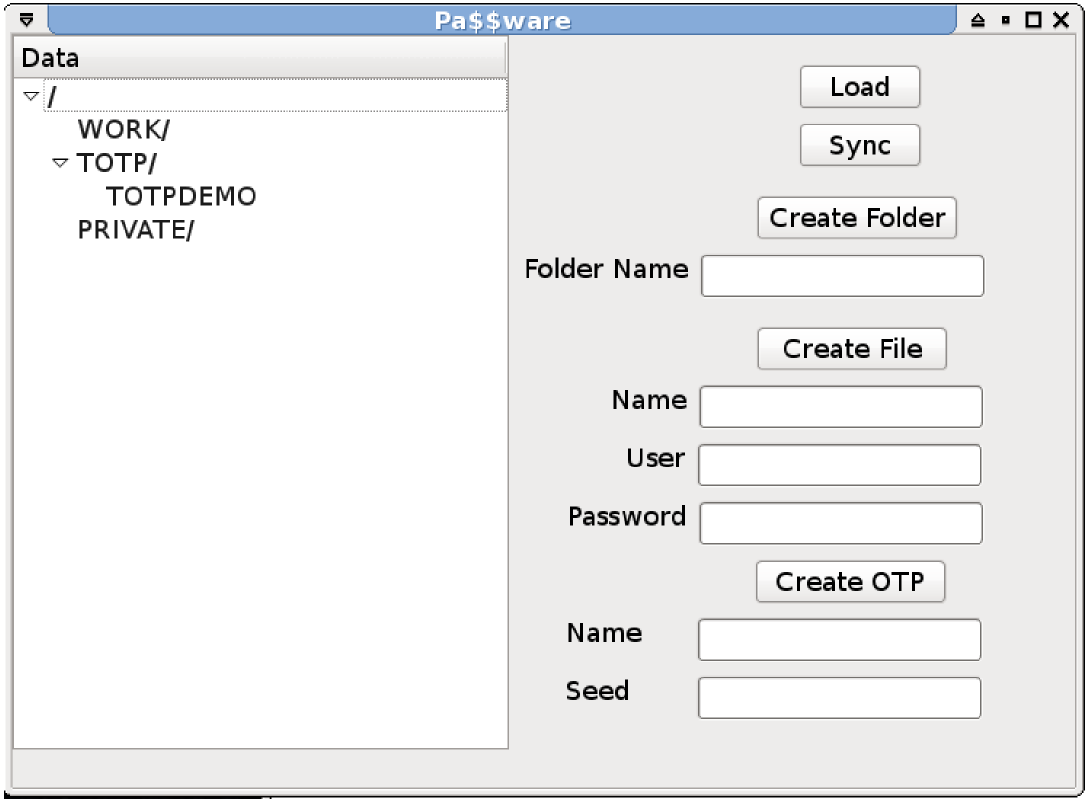
- The app's link uses a serial communication with the Teensy
  - You have to enable serial communication on the device to allow access
  - You are only allowed to push new data
    - You cannot access the password using this link
  - The link is also used to synchronize the RTC

Communication protocol

- Very simple communication protocol
- Two modes of communication
  - Normal mode
    - USB HID
    - Unidirectional communication : Pa55ware to PC Only
  - Command mode
    - USB Serial communication with 9600 bauds rate
    - Bidirectional communication

Desktop client

- Developed with Python 2.7 and QT 4
- Used to create and update value
- Works only with the command mode



Desktop Client communication

- Pa55ware starts sending \x42\x42
- The client can send its own command
- Example of command for listing root directory
  - \x04\x01/
- Example of command for setting a username
  - \0x1\0x11\0x5/toto\x01\x01\x08password

Demo !

Roadmap

- Now in beta version
  - Basic functions working
  - Code will be released after Passwordscon
- First stable release in January
  - Add a random IV for each AES stream
  - Use the hardware fuses to protect the EEPROM in case the Teensy is flashed
  - Fix the communication protocol and file format

Future improvements

- Password generator
  - I think the capacitive inputs make a good source of entropy
  - Wave your hand above the device to generate a random password
- New OTP protocols
  - HOTP

Future improvements - cont

- File storage
  - Need to wait for the USB storage function support in the Teensy core library
  - Would allow support for SSH identity keys

Why are we here ?

- This project needs to be audited
  - We may have made logical mistakes
  - Maybe there are bugs ?
- We suck at crypto
  - We think we did well, but we may be wrong
- We have basic knowledge of hardware hacking
  - Maybe there are ways to extract data

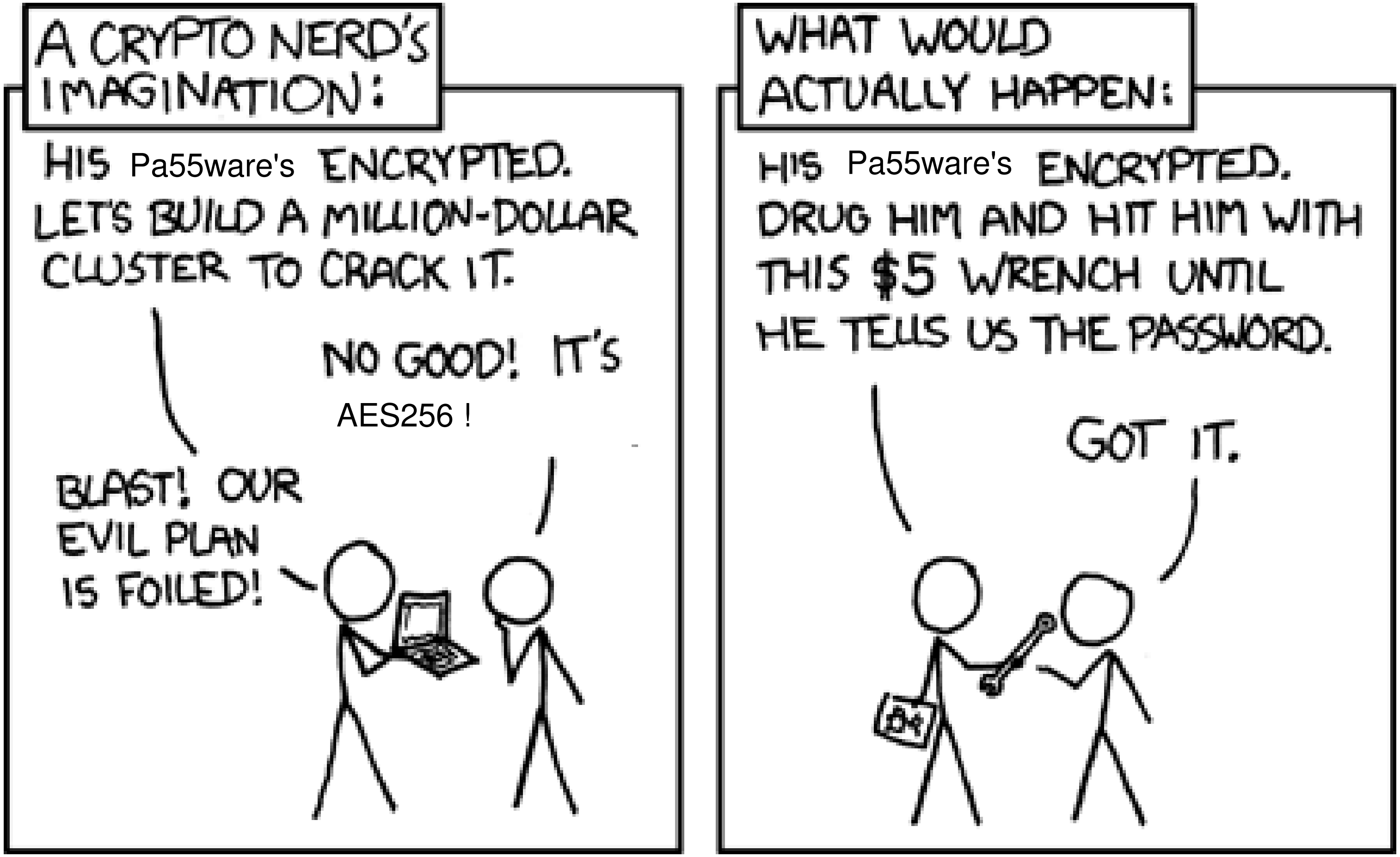
We need you !

- People here are more than qualified to spot our mistakes and improve this project
- YOU can help make this
  your new password manager !

That's all !

- Any questions ?
- Feel free to come and see Pa55ware live

Don't forget


A CRYPTO NERD'S IMAGINATION:
HIS Pa55ware's ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S AES256 !
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS Pa55ware's ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

http://xkcd.com/538/

Thank you !

- Nicolas Oberli
  - @Baldanos
  - http://www.balda.ch
- Manoé Zwahlen
  - @0xsata