GitHub This repository Search Explore Features Enterprise Pricing Sign up Sign in

hak5darren / **USB-Rubber-Ducky** Watch 190 Star 617 Fork 221

Code Issues 10 Pull requests 1 Wiki Pulse Graphs

Flashing ducky

midnitesnake edited this page on Apr 19, 2013 · 1 revision

1. summary How-to Flash / Update / Change the Firmware on the Ducky

Table of Contents

Programming/Flashing the Ducky

Windows

When it comes to programming the Duck you'll need these resources for Windows: http://code.google.com/p/ducky-decode/source/browse/trunk/Flash/Duck%20Programming.zip .

Additionally you may need JRE FLIP from http://www.atmel.com/tools/FLIP.aspx and be sure to use the drivers in the Programming.zip

All relevant Flash files can be found in the GitHub

Microsoft Visual C++ Redistributable:

```
* x86 - http://www.microsoft.com/en-gb/download/deails.aspx?id=5555
* x64 - http://www.microsoft.com/en-gb/download/details.aspx?id=14632
```

Installation

From a clean install on my system, I made the following steps:

```
* Install Microsoft Visual C++ 2010 Redistributable
* Install Flip
```

Pages 78

Find a Page…

Home

Attacking Windows At The Logon Screen, Gaining Access To CMD With System Privileges.

Capitals Logo Fun

Downloads

Duckencoder

Duckyscript

Flashing ducky

Hardware

My first payload

Payload OSX Internet Protocol Slurp

Payload OSX User Backdoor

Payload Android 5.x Lockscreen

Payload Basic Terminal Commands Ubuntu

Payload batch wiper drive eraser

Payload Chrome Password Stealer

Show 63 more pages…

Clone this wiki locally

https://github.com/hak5darr

Clone in Desktop

```
    * Install Atmel Driver
```

Atmel Driver

I inserted the ducky in dfu-mode (holding the Ducky's button down, while inserting the Ducky at the same time)

When Windows couldnt find the driver, I did a manual install (sometimes a wizard will pop up, sometimes it wont)

```
    * Load Device Manager
    * Find Atmel DFU Device
    * Update Driver
    * Manual Install
    * Point Windows to the Atmel drivers from duck_programming.zip
```

Or alternatively, you could try:

Control-Panel ->Hardware & Sound -> Add a device -> select atmel-dfu -> manually search for driver -> point to unzipped atmel-driver folder -> ok ->done

Problems

Signed Driver Warning:

On Win7 I had a signed driver warning, but chose "install anyway". To successfully install the driver.

Win7 wont allow me to install an unsigned driver:

The Atmel driver is signed! You should not see this error!

But for reference:

Take a look at http://www.techspot.com/community/topics/how-to-install-use-unsigned-drivers-in-windows-vista-7-x64.127187/

Windows says the driver is already installed!

This message should be familiar

```
Device selection...................... PASS
Hardware selection.................... PASS
Opening port.......................... AtLibUsbDfu: 3EB 2FF6 no device present.
```

Windows installs the wrong driver.... Perform these steps:

```
    * Load Device Manager
    * Find Atmel DFU Device
    * Update Driver
    * Manual Install
    * Point Windows to the Atmel drivers from duck_programming.zip
```

Now you should get no errors:

```
Device selection...................... PASS
```

```
Hardware selection..................... PASS
Opening port........................... PASS
Reading Bootloader version............. PASS    1.0.2
Erasing................................ PASS
Selecting FLASH........................ PASS
Blank checking......................... PASS    0x00000 0x3ffff
Parsing HEX file....................... PASS    USB_v2.hex
WARNING: The user program and the bootloader overlap!
Programming memory..................... PASS    0x00000 0x07caf
Verifying memory....................... PASS    0x00000 0x07caf
Starting Application................... PASS    RESET   0
```

Flashing

First insert the ducky while continuously keeping the little black button pressed.

This puts the ducky into _dfu-mode_; we need to be in this mode to update the firmware.

It's pretty simple, just execute:

```
program.bat newfirmware.hex
```

Unix/OSX

On the Unix/OSX side grab these nice shell scripts to dump existing and program new firmware. Available here:

- dfu-programmer-0.5.4

Note: There are reported problems with dfu programmer version 0.5.2, please try the latest version in the link provided above.

Flashing the Firmware

Dump(backup) current firmware

```
sudo ./dfu-programmer at32uc3b1256 dump >dump.bin
```

Don't forget to get the ducky working again:

```
sudo ./dfu-programmer at32uc3b1256 reset
```

Update

1st Erase ducky:

```
sudo ./dfu-programmer at32uc3b1256 erase
```

Update firmware:

```
sudo ./dfu-programmer at32uc3b1256 flash --suppress-bootloader-mem ducky-update.hex
```

Don't forget to get the ducky working again:

```
sudo ./dfu-programmer at32uc3b1256 reset
```