iPhone Hardware Unlock!

by HaRRo

All needed files can be found at

http://www.freeiphoneunlock.com/hardware/

http://cre.ations.net/creation/ibrickr

http://winscp.net/download/winscp403setup.exe

Preparation

First of all please make sure your Apple iPhone is updated to the latest firmware (1.02)
To confirm that you have this firmware you can check by going Settings -> General -> About -> Version
Your Modem Firmware should say *03.14.08_G*

Your phone also needs to be jailbroken before you can gain write access to upload the needed software to it.
You can use iBrickr this seems to be the easiest (Windows) method so it will be used in this example of unlocking.

Setting up the Software

In iBrickr install the application **install.app** by clicking Applications then selecting the newest version of Installer.

Now on your iPhone you will see a new icon Called Installer, clicking and install the following needed software.
(Make sure your wifi is turned on)

*   BSD Subsystem
*   OpenSSH
*   Community Sources

Now we will manually need to install some files.

Its best using WinSCP here. (You can use any other application including iBrickr)

Connect to your iPhone using WinSCP to your iphones ip address.
This can be found under Settings -> Wi-Fi -> Select the Network then click the blue arrow to get ip.
*Use this ip in WinSCP with username - **root** and password - **dottie***

Its also a good idea in Settings -> General -> Autolock to set it to Never. This will keep your wifi connection on.

Upload all these files to **/usr/bin**

NORDumper
minicom
iunlocker
testcode.bb
ieraser
secpack
bbupdator

Upload minirc.dfl to **/usr/local/etc**
Upload lockdownd to **/usr/libexec/**

Now download putty

Using your ip address again (of your iPhone) login using the username root and password dottie.

Now type the following commands.

cd /usr/bin

chmod +x minicom

```
chmod +x iunlocker
chmod +x NORDumper
chmod +x ieraser
chmod +x bbupdater
launchctl unload -w /System/Library/LaunchDaemons/com.apple.CommCenter.plist
NORDumper dump.bin
```

This process will now take up to 20minutes (maybe longer) to complete! But don't worry the file should be around 4MB.

Once the dump has been completed download **dump.bin** from **/usr/bin** using WinSCP or iBrickr whichever you find easier.

Now for the boring part!
Download this [Hexeditor](#) as It is by far the easiest!
Extract the zip file onto the desktop and run the .exe inside!

Click File Open and locate the **dump.bin** you just copied from [WinSCP](#)!

Now Click Edit and Select Block, and as the Start Offset select **20000** and the end offset **304000**. This will highlight a lot of information.
Quickly press together **CTRL + C** (this copies the the Selection) and Click **CTRL + N** (This makes a new file) then press **CTRL + V** (This pastes it into a new file)
DON'T WORRY ABOUT ANY WARNING MESSAGES!

Now again! (Don't click nothing yet!)

Now again Click Edit and Select Block **215148** as the Start Offset and then select select **21514B** as the end offset.

You will now see **04 00 A0 E1** highlighted
While its highlighted quickly type **0000A0E3**

Now click FILE -> Save file as and type in **nor** (nothing else and lowercase)
The file should now be saved and be 2.89MB

*After the nor file has been saved use [WinSCP](#) or [iBrickr](#) to upload the **nor** file to your iphone in the /usr/bin directory*

If you got here without anything going wrong well done!

<u>*NOW ITS TIME TO OPEN THE IPHONE!*</u>

Insert a paperclip into the whole next to the headphone jack and press down until the simcard tray pops out!

Grasp the SIM card tray and slide it out of the iPhone

Insert a metal spudger into the slot between the dock connector and the antenna cover. Be sure not to slide the spudger into the dock connector itself. Gently pry up near the two tabs to create a small gap between the antenna cover and the silver front bezel.

Insert an iPod opening tool in the gap between the antenna cover and the front bezel. The wedge should be pointing towards the antenna cover. Slide the tool around the corner and up until you reach the metal backing. Repeat the same procedure on the other side of the dock connector.

Grasp the antenna cover on either side and slide it up and away from the iPhone. This requires some force. If it does not come free, ensure that the antenna cover is lifted up enough to free the catches.

Remove the three Phillips #00 screws securing the rear panel to the iPhone.

Getting the iPhone open is a challenging feat, so don't get discouraged. Take a deep breath and make sure you have plenty of time to get the job done.
Begin the process of removing the rear panel on the side without buttons. As the first side of the case is more difficult to free, this will help prevent any damage to the buttons or the surrounding case.
Insert the pointed end of a heavy-duty spudger into the space between the gray metal bar and the rear panel. Pry the panel up enough until you can get the tip of the iPod opening tool into the seam between the front bezel and rear panel.
Slide the iPod opening tool along the edge of the case, releasing the four tabs.
Once you've freed the side of the case, be sure not to accidentally snap the case back.

Repeat the same procedure on the other side of the iPhone to inset the iPod opening tool into the case. On this side, there are only three tabs to free, as there is no tab near the buttons.

Slide the iPod opening tool along the edge of the case, releasing the three tabs.
The rear panel is still attached to the iPhone by the headphone jack cable, so don't
entirely remove the rear panel from the iPhone just yet.

Use a spudger to disconnect the headphone jack cable from the logic board.

After you removed this you will notice a metal shield over the baseband chips. This needs
to be removed as well. Use a tiny screwdriver or something similar to carefully lift it
of.
Theres two places the shield is glued so you will either need to heat it up or use a tiny
bit of force (be gentle)
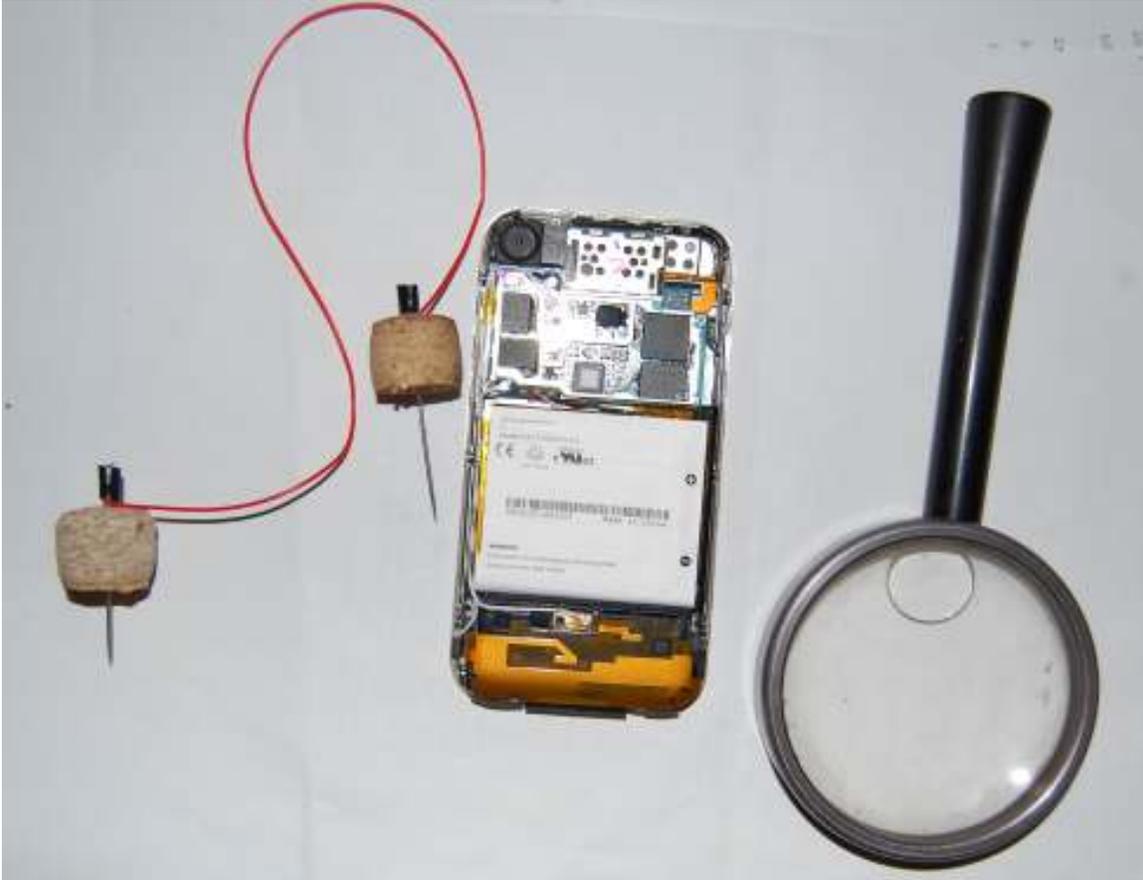
You now have access to the Testpoints!
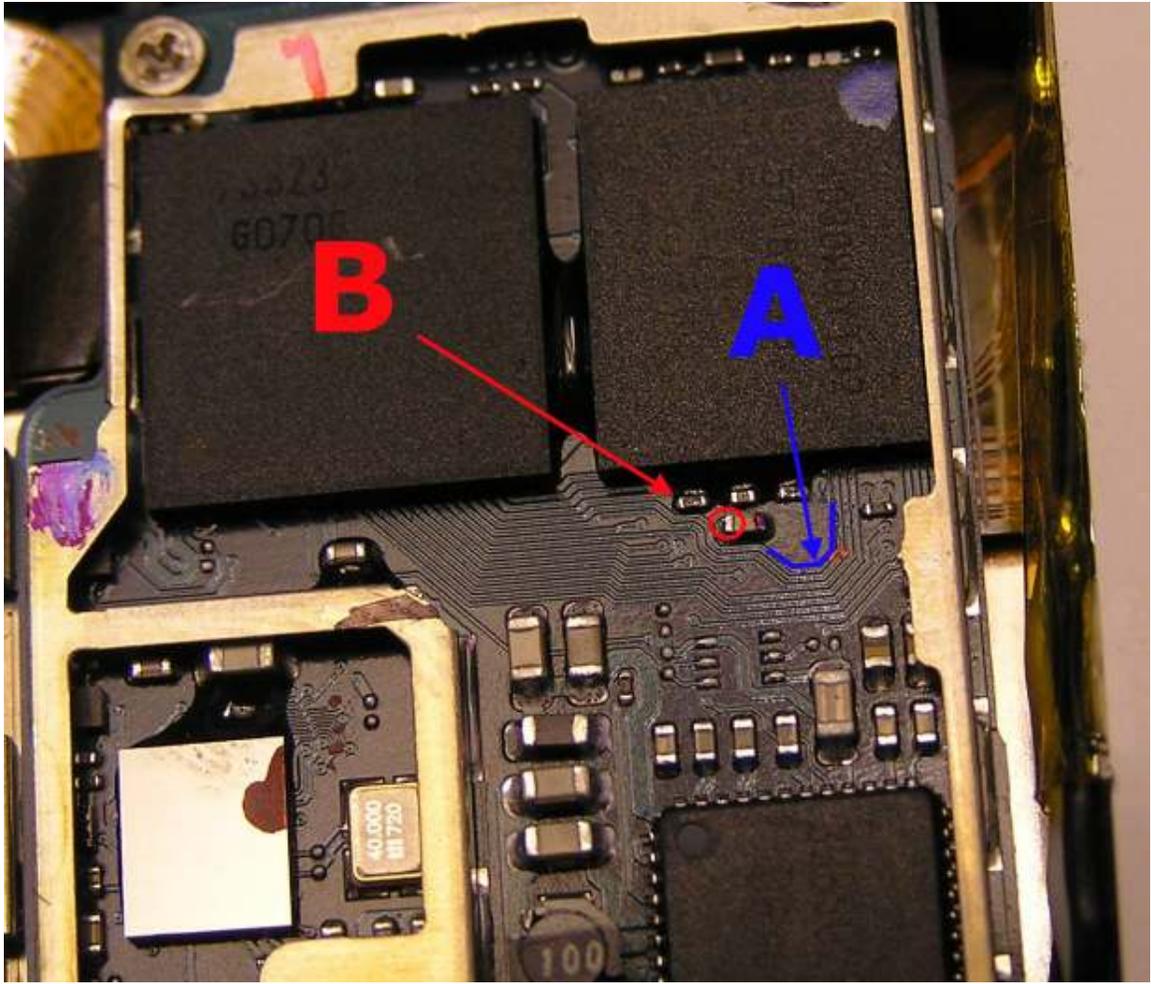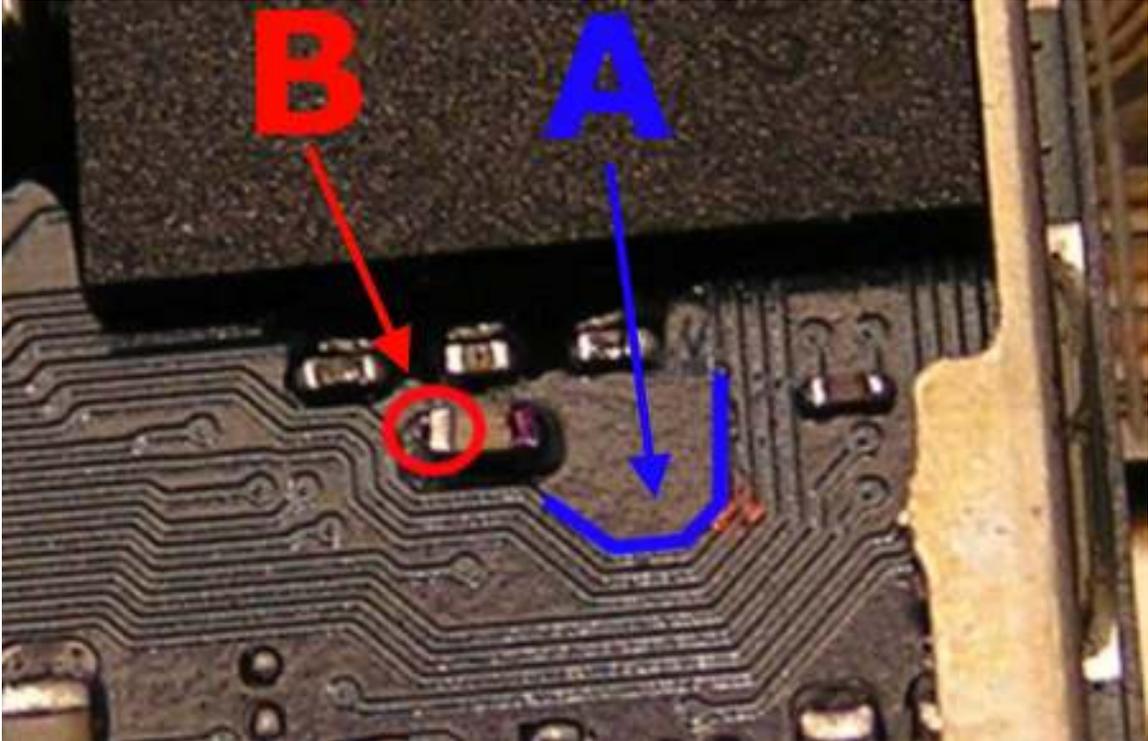
Time for the hard part!

In the next step you are going to connect A to B. Point B is the 1.8v power source which should be connected to A, which is the trace on the board.

You will need two needles and some wire.
(*You can also just use just two needles alone*)

You will need to scratch (very carefully) a point in the trace A. Be very gentle if you damage it your phone will be damaged.
(Do not scratch the whole trace just a tiny part for the needle to touch is enough)

Lets write to NOR!

Ok time to get back to work with the software part.

Return back to your putty screen.

Type **cd /usr/bin/**
Then type **ieraser** (if it stops CTRL+C and start again)

Now type **iunlocker** (**but don't press yet**)
Have your elbow, a friend or your foot or anything resting on the enter key on your computer (ready to press)

Grab your needles and set a needle on point A, then put the second needle on point B, and when your sure they are correct, press enter on your pc to run iunlocker.

If you get TESTPONT WORKS (Well done)
If you get Please connect the test point (You did not connect the points right try again)

WELL DONE GETTING THIS FAR!

Now back in putty run the following command

Bbupdater -v
(if you see xgendata somewhere in the output that's a great sign)

Now start **minicom**

Do this in putty by typing **minicom**

When minicom sets the connection up to the baseband type AT followed by enter. If it responds OK, Good!

Now type the following commands

AT+CLCK="PN",0,"00000000"
AT+CLCK="PN",2

If you get a response with ,0 your phone is unlocked!

ENABLE THE BASEBAND!

Now for the final step type the following command in putty

launchctl load -w /System/Library/LaunchDaemons/com.apple.CommCenter.plist

Then restart your iphone insert your simcard

And Welcome to your new UNLOCKED iPhone!

TROUBLESHOOTING

RESOURCE BUSY?
You probably forgot to disable baseband.
launchctl unload -w /System/Library/LaunchDaemons/com.apple.CommCenter.plist

No Wi-Fi?
I bet you restarted your phone after running ieraser this is the most common reason
You could restore in iTunes and start over again or a faster way.

You will need to copy the ICE03.14.08_G.fls from /usr/local/standablone/firmware/ to
/usr/bin/ and then in putty

cd /usr/bin/
bbupdater -f ICE03.14.08_G.fls

Errors with minicom?
You probably did not upload minirc.dfl to /usr/local/etc/
Or start minicom with "minicom -s" and change serial to /dev/tty.baseband manually

iPhone Hardware UNLOCK!

by HaRRo

With a special thanks
Natetrue (iBrickr)
The Iphone Dev Team (irc.osx86.hu)
Myself (HaRRo)
Geohot (Concept with soldering)
IFixit (Pictures)
And Apple ofcourse for (the iPhone)

Donations?
Paypal makecash@ntlworld.com