

IPOD TOUCH JAILBREAK

By Shaun Lee|Slip

CONTENTS //

IF YOU HAVE 1.1.2/1.1.3	1
JAILBREAKING 1.1.1	2
UPDATING TO 1.1.2	2
BSD SUBSYSTEM	3
IPHONE APPS	3
SFTP	3
SUMMERBOARD	4
CUSTOMIZE	5
RELOCATING APPS FOLDER	6
GLOSSARY	7
SPECIAL THANKS	9
DISCLAIMER	9

Note: this guide is Mac specific as I have not tested them on a PC and also the added complexity of writing for both platforms. Anyone wanting to alter it for PC's, feel free.

IF YOU HAVE 1.1.2/1.1.3 //

If you are running on the 1.1.2/1.1.3 firmware you will first need to downgrade to 1.1.1. This is due to the hole that the jailbreak was using to do the jailbreak was plugged in the later firmware releases.

To do this, download the [1.1.1 firmware](#) to a place where you will remember, preferably the Desktop. If you are using Safari then turn off the Auto Open Safe Files option in Preferences.

Once the file has finished downloading, rename it so that the .zip is removed leaving you with a file ending in '___Restore.ipsw.' It will ask you if you want to use .zip or .ipsw, choose .ipsw. If done correctly then the icon should change to a lego block with an iTunes and iPod icon on it.

To downgrade your iPod it needs to be in restore mode. To do this, plug it into your Mac, start up iTunes if not already and then hold down the Lock/Wake button and Home button simultaneously. Keep them held down until your iPod shuts off, keep the buttons held down and when you see the Apple logo, let go of the Lock/Wake key ONLY, leaving the Home key pressed down and eventually you should get the iTunes logo with a picture of a USB cable.

iTunes should now say it's detected an iPod in Recovery Mode; click OK, hold down the Option key and then press Restore and point iTunes to the .ipsw restore file on the Desktop. It should now start restoring to 1.1.1.

JAILBREAKING 1.1.1 //

Now that your iPod is running 1.1.1 you can now actually jailbreak it. To do this, point the touch's Safari to www.jailbreakme.com, scroll down to the bottom of the page (you can read through the FAQ's if you are interested in what it specifically does) and click on Install AppSnapp and soon after, Safari will 'crash'. If you wait, your iPod will start to auto jailbreak. This can take a few minutes so be patient. Once this is complete it will ask you to slide to unlock. Once you have unlocked you should see a new icon on the Home screen called Installer.

UPDATING TO 1.1.2 //

Now that the iPod is jailbroken we can now update to the more recent 1.1.2 firmware which fixes a series of bugs and inconsistencies. To upgrade to 1.1.2, go to the new Installer app, go to the Install tab and scroll down to '1.1.1 Tweaks' and install Oktoprep. Click the Home button and it will ask you to slide to unlock. Once installed, download the 1.1.2 restore file [here](#). Once the file is downloaded, rename the file so that the .zip is removed and so you have a file ending in '_Restore.ipsw' as before. Open up iTunes, plug in the iPod and then hold down the Option key and click Update in iTunes and navigate to the 1.1.2 firmware file you downloaded.

Once iTunes has finished updating, grab the [1.1.2 jailbreak](#) program and extract to the Desktop. Run the application called Jailbreak.jar, check the 'Install SSH' option and then click the Jailbreak button. When this has finished jailbreaking, power off your iPod then turn it back on, your iPod will reboot when loaded up (this is normal) when its rebooted you will then have a jailbroken 1.1.2 iPod touch.

BSD SUBSYSTEM //

Once finished it's best to install the BSD Subsystem. This allows for many apps to be installed and run such as the Apollo IM app and also if you decide to do any more advanced procedures. To do this go to Installer → Install → System → BSD Subsystem → and then tap Install.

Once it has finished installing, slide to unlock and all is done.

This is one of the most important packages to install and so is highly recommended .

IPHONE APPS //

Due to the iPod having near identical hardware and software to the iPhone it is possible to run the iPhone apps on the iPod. To install the iPhone apps you will need to add a new Source to Installer. To do this, touch the Installer icon, tap the Sources tab in the bottom right hand corner and then hit Edit in the top right corner. In the top left corner tap Add and enter this URL: <http://applerepo.com>.

Once added, go back to Install and scroll down to iPhone apps 1.1.2.

For the Mail and Maps application you will need to install the Prep files before you install the app.

SFTP //

Secure File Transfer Protocol, more commonly known as SFTP or SSH, is a way to transfer files to the iPod touch using WiFi. If you remember, when we jailbroke 1.1.2 we installed OpenSSH. This sets up the iPod so that it can accept SFTP connections and allows you to transfer files to it.

The best way that I have found to transfer files and access the iPod is a program called AFPd. It allows you to access your iPod as if it was a remote computer through Finder which means it shows previews of images and files whereas other programs simply list the files.

To install this program, follow [this](#) guide.

Now that we know how to transfer files to the iPod, you may be wondering what we can actually do with this new found knowledge and hopefully the next section offers an example of what you can use it for.

SUMMERBOARD //

SummerBoard is an application that allows you to customize the iPod's SpringBoard, that is, the icons you see on the Home screen, the wallpaper that appears behind them and the Dock image that the four icons sit on. It also allows for more than one page of icons to be used so that you can have more than 16 icons on the Home screen.

You will need to download SummerBoard through Installer (under System). Note: the application on the Home screen will be named SMBPrefs.

To change how the iPod looks you will need to do the following things. To change the icons, wallpaper and dock you will need a 'theme' that SummerBoard can use. You can download pre-made ones from Installer under 'Themes (SummerBoard)'. However, you can also create your own, custom, themes by creating a themes folder that you can upload to the iPod.

This theme folder will include all that is needed for your custom theme but before we get started you will first need to decide what you want to call your theme and then create a new folder on your Desktop with that name. In that folder you will need three things. If you want to change the wallpaper from the original black then you will need to include a file called 'Wallpaper.png'. This file will need to be a 320x480 PNG file. If you do not want to use a custom wallpaper and want to keep the black background simply don't include a wallpaper file.

The second thing you will need is a Dock image. This image will be used as the custom Dock image that the Dock items will sit on. This file will need to be 320x91 and like the wallpaper, will need to be a PNG. You can use any amount of opacity to create different looks or go fully transparent if you want no dock to show up at all. Again, like the wallpaper, if you like how it is then don't include a 'Dock.png' file. Lastly we will need a folder for the icons to go in. Create a folder inside your theme folder and name it 'Icons'. Your icons will need to be 60x60 or smaller PNG's and can be any shape and size that you wish. If the application icon that you want to replace is, say, Safari, then the icon image should be named 'Safari.png'. This applies to all icons on the Home screen eg, Music would be 'Music.png'. Note: all file names in SummerBoard are case sensitive and so for example 'music.png' will not be the same as 'Music.png'. You will need to type them in as I have shown.

Now that we have the theme folder all made we will need to get it on to the iPod to be used. To do this we will use SFTP that we learnt about earlier. To upload the file, connect to the iPod through Finder and then navigate to to: Root's Home/Library/SummerBoard/Themes. In the Themes folder you will see all of the themes currently

installed . To add yours to the folder, simply drag the folder from the Desktop into the Themes folder and it will be copied across.

Once uploaded we will need to set SummerBoard so that it uses our new theme. To do this, open up SMBPrefs, tap Theme and then tap Your_Theme_Name_Here and then it will take you back to the previous page. Scroll to the bottom and hit 'Restart SpringBoard' and wait from anywhere few seconds to half a minute. After the delay it will lock and ask you to slide to unlock and when you do, you should see your new theme set.

CUSTOMIZE //

Customize is an application that allows you to reorder icons on the Home screen to your own taste. To install it requires a little trial and error plus a bit of patience but the best way I've found is to download and install via Installer (it's listed under Utilities), hit the Home button and slide to unlock but do not open it once it is downloaded. What you will need to do is go back to Installer, scroll to 'Themes (Customize)' and then install any theme you see, it really doesn't matter. Again, hit the Home button, slide to unlock and this time we can actually open it. Tap the Customize icon and it should load up after a little delay and (if successful) you should see a list of options. If it fails to open, go to Installer, uninstall and reinstall Customize and repeat the process mentioned (you shouldn't need to uninstall the theme though I haven't tested it as it worked first time for me). If however it did work, you should see a list of options that are not specific to the iPod such as Bluetooth setting. Ignore these and tap 'Icon Display Order' → 'Manual Reorder' and then you should see a list of all of the apps that you have installed.

There are two section on the list, 'Dock' and 'Spring Board'. Any icons that are under Dock will, unsurprisingly, appear in the Dock. All of the other icons will be on the Spring Board in the order that you set. So say for example, if you want Calendar to appear as the first icon on the Home screen then you would drag the Calendar icon to the top of the list by grabbing on to the three stacked hyphens on the right of the screen. You can then carry on rearranging the icons as you wish. If you want the Calendar icon to appear as the first item in the Dock then all you would do is as before but carry on dragging it until it is listed under 'Dock'. Note: the icons on the Home screen run from left to right, top to bottom and so the fifth icon in the list will appear on the second row of icons on the far left.

You can also set whether the icon of an app shows up at all on the Home screen. For example, OpenSSH is installed when jailbreaking and you may not necessarily want

to uninstall it but may also not want to have it's icon on the Home screen all the time and so to hide it, go to Display Order as before and then hit the eye icon in the top right corner. This will cause all of the grey eye icons to the left of the application icons to turn black. You can now tap any icon in the list so that the eye next to it disappears meaning that once the SpringBoard is restarted, that icon will not be visible. Once you are done adjusting the visibility you just tap the eye icon in the top right corner again.

Once you have the icons set as you like, hit the Home button and it will restart the SpringBoard (just like SummerBoard does, though a lot faster). Slide to unlock and you should see all of your icons in the order you set with the icons that you set as invisible will be, shockingly, invisible.

You can also set how many icons sit in the Dock by going to Icon Display Order → Number Dock Icons and then choosing how many you want. It will instruct you how to apply the setting.

RELOCATING APPS FOLDER //

Pretty soon after you start installing applications you will start to see low memory warnings appear. This is due to all of these new apps being installed into the System partition of the iPod's memory which is a 300MB partition which houses the firmware and the standard applications (which sit in the 'Applications' folder). The other partition is the remainder of the memory which is used for all of your music and videos etc. and is called 'Media'.

As mentioned, after you start installing apps (depending on size) you will soon start to fill up this System partition and so will not be able to install any more new apps. To get around this problem it is required that you move the Applications folder to the Media section where it can be as large as it needs, memory permitting, leaving the firmware and other important files behind in System.

When we move the Apps folder to the Media section, a link is set up so that the iPod thinks that all of the applications are in their original location and is none the wiser.

There are two ways in which to relocate the Apps folder. The easiest and most recent way to do it is with 'BossTool'. It basically automates the entire procedure and involves no skill whatsoever. There is a full write up and tutorial [here](#). If, however, you would prefer to do things manually and see what commands are being run, then you can follow [this](#) guide. However, due to actually having to type

the commands and the potential for error, I would recommend the BossTool app for all of those who aren't so fussed with the behind-the-scenes methods.

Note: the BSD Subsystem is required for this to work.

GLOSSARY //

Not all of these terms apply to the iPod touch but they're worth noting. Ones which apply to the iPod touch as well as the iPhone are marked in red.

Accelerometer – A tiny 3-axis device that monitors the iPhone's position in its environment. Basically it can tell which way it is being held or rotated.

Activation – The process that allows you to move beyond any of the various screens that instruct you to connect your device to iTunes before it can be used. On the iPhone, you can only make emergency calls until your iPhone is activated. Out the box, the iPhone doesn't do much except look pretty and make emergency calls. Activation gives access to normal operation. Typically this is accomplished using iTunes, by obediently signing up for service with official carrier AT&T. But if the world comprised of only obedient people, we wouldn't be here today. With buggered-up iPhones.

Baseband – The part of an iPhone's memory that provides the firmware for the phone's radio modem chip.

Bricking – To render an iPhone inoperable. The 1.1.1 firmware update turned many iPhones into iBricks. Users could not reactivate their iPhone to get past their "Please connect to iTunes" screens. Although the phones could still be used for emergency calls, users were locked out from all normal iPhone operations. Note: it is impossible to brick an iPod touch, every problem you can run into can be solved by restoring in iTunes.

DevWiki – The developer wiki for iPhone is hosted at iphone.fiftyfour.net. Many developer projects first appear here and the site contains a wealth of iPhone and iPod touch related information. The iPod touch Developer Wiki contains many of the most important recent developments regarding the touch. The phrase DevWiki may refer to either of these two sites.

/etc/fstab – The file on your iPhone or iPod touch that states whether your file system allows read-write access.

Emulator – A program that allows a computer or modern console to emulate a video game console.

File system – The way your iPhone or iPod touch uses its memory to store data and applications. The iPhone and iPod touch use two "disks": a smaller private file system that contains the operating system and a larger public one that contains your media (songs, videos, etc), preferences, and data.

Firmware – the iPhone and iPod touch's built-in programming, embedded into memory set aside for this purpose. Apple releases periodic updates to this code, and it's a combination of earlier unauthorized modifications and official update number 1.1.1 that led to the current "iBrick" situation. To hardware grognards, the dangers of injudicious firmware fiddling are well-known but

Apple's made the process of updating simple and straightforward — at least for those who toe the line.

GSM – Global System for Mobile Communications, a popular mobile phone standard used by the iPhone.

Hacks – This refers to all the adventures herein, be they baffling text commands or GUI applications. So called “jailbreaks” provide beach-head access to the system in juicy anticipation of further hacking. Other hacks activate the phone for general use without forcing the user to go through the official process. Others unlock the phone from AT&T's mobile network (two popular examples are iPhoneSimFree and AnySIM), while others make easy the installation of unofficial software.

Jail – The public areas of the iPhone or iPod to which, by default, Apple allows read/write access via USB. In Unix terms, this refers to the `/private/var/root/Media` folder.

Jailbreak – The iPhone and iPod touch hacks that allow users to gain access to the entire Unix filesystem. In Unix terms, this refers to changing the root of the directory tree to. A hack can also consist of being able to access to areas of the iPhone that users aren't supposed to mess with. Typically, this is an immediate prelude to either installing cool programs, unlocking the handset for use with another cellular network, or both.

SIM lock – A limitation imposed by the manufacturer of a GSM phone to limit a phone to certain carriers. The US iPhone is SIM locked and can only be used with AT&T.

SpringBoard – iPhone and iPod touch's default application launcher. Basically this is the stock software that runs your home screen where you launch all your applications.

SSH – Secure SHell. This is a shell that runs on your iPhone or iPod touch using port 22 and allows you to connect wirelessly to a Unix shell. It basically allows you to transfer files to the iPod via WiFi.

Third party apps – iPhone and iPod touch applications that were neither created by nor commissioned by Apple. So-called “native” apps are faster, better, and allow access to iPhone functions that Safari does not. Many iPhone users are happy with official carrier AT&T and hack their handsets simply to run these programs.

Toolchain – In terms of the iPhone/iPod touch world, a compiler and linker developed by Patrick Walton of the University of Chicago and his compatriots. It allows developers to create applications that can run on the iPhone and iPod touch's ARM processor.

Unlock – Bypassing a phone's SIM lock to allow it to be used with any carrier with compatible equipment. In the US, the iPhone is compatible with both AT&T and T-Mobile's GSM equipment. You can often pay a premium to buy a phone untethered to a particular carrier. Apple's iPhone is not such a phone. Apple developed powerful and complex locking systems to prevent you from leaving AT&T's cold embrace. Though unofficial unlocking solutions soon arrived, it was these unlocked iPhones that faced the worst problems after Apple's official 1.1.1 firmware update.

SPECIAL THANKS //

I would like to pay a special thanks to the [Apple iPhone School](#) for their Glossary that they so kindly let me use, it really is a wonderful site; take a look!

I would also like to thank Andybno1 from [MacForums](#) who let me use his jailbreak tutorial as the backbone of this guide.

And of course, the wonderful work of all of the hackers that work on these apps and jailbreaks for no pay apart from our enjoyment, you wouldn't be reading this without them. And remember, if you enjoy any of these apps donate! It really does help keep the project going.

DISCLAIMER //

Due to the unofficial and unsupported methods in this guide, they come with a fair degree of risk. Most of the topics here I have either personally used or are widely documented and so am confident that, nine times out of ten, they will work. However, since I didn't write any of these apps or compose any of more advanced tutorials, I can't offer any type of guarantee or promise. You may be that one person out of ten that doesn't work and so in short, use at your own risk.

Just keep in mind, if anything does go wrong then you can always just restore through iTunes and it will erase all of the hacks and modifications made leaving with you with a factory fresh iPod. You also can't, contrary to popular myth, brick an iPod; it is only possible with an iPhone. You may think that you have bricked your iPod but it can sometimes take up to 20 restores to get it back, just hang in there and keep trying.

If you have found this guide useful, feel free to distribute it, copy it, change it, link it, whatever. I would, however, appreciate if you would note or at least mention it was written by me and/or a little credit as it took quite a while to get all of the links, guides and my own grammar in place ;-). And oh, if you feel an overwhelming need to donate, pick you're favourite charity and give them my love.

If you would like to get in contact, feel free. Just drop me a line at shaunmlee@hotmail.co.uk.

PS. Enjoy your jailbroken iPods ;-)