THURSDAY, AUGUST 23, 2007

Step 8

Now its time to patch the firmware. Thanks to gray for finding these patches, this required some very complicated reversing.
First, you need to extract the firmware from your nor dump. The range you need is 0x20000-0x304000. Save this file as "nor".
The patches you need to apply are as follows. These are offsets from the begininning of the file to saved as "nor". Choose your version, and patch.
3.12: (213740): 04 00 a0 e1 -> 00 00 a0 e3
3.14: (215148): 04 00 a0 e1 -> 00 00 a0 e3
Resave the file nor, you'll need it soon...

POSTED BY GEORGE HOTZ AT 2:44 PM

6 COMMENTS:

lesterine said...

im confused? are you using a regular hexeditor to extract the 0x20000-0x304000 range from the nor dump?

AUGUST 24, 2007 3:29 AM

Brownie Girl said...

Good job! You will be rich very soon! Here's a link that let me get one free ringtone 4 my iphone - no subsription required - but it only give u one free :(

http://ushrink.com/freeringtone

AUGUST 24, 2007 2:11 PM

pk said...

How to contact you? pl contact me I need to sell it on my www.talkfree7.blogspot.com

Thanks,
ingp55@yahoo.co.uk

AUGUST 25, 2007 5:10 AM

john said...

Great news guys,CONGRATULATIONS!
Now you will be able to use global sim card with IPhone. Check it out at www.1world1sim.com, card comes with free roaming charges and service around the world. Free incoming calls in

charges and service around the world. Free incoming calls in more then 70 countries.

AUGUST 25, 2007 11:07 AM

indiekiduk said…

This post has been removed by the author.
AUGUST 25, 2007 8:33 PM

Zebrum said…

cant get it to work in the UK with this patch. can activate sim but get no service on vodafone and o2. Perhaps we need another patch?

AUGUST 25, 2007 8:34 PM