Step 7

So here is the first tool release, iEraser. This erases the current firmware on your modem. Don't worry, you can always put it back with bbupdater. Here how the bootrom check works; it reads from 0xA0000030 0xA000A5A0 0xA0015C58 0xA0017370 and all these addresses must read as blank, or 0xFFFFFFFF. When you erase flash, it becoms 0xFFFFFFFF. But you can't erase those locations, because they are in the bootloader. So thats where the testpoint comes in. Pulling A17 high hardware OR's the address bus with 0x00040000(offset one because data bus is 16 bit) So the bootrom instead checks locations 0xA0040030 0xA004A5A0 0xA0045C58 0xA0047370, which are in the main firmware and can be erased. Pretty genius :)
To use this tool, you need the secpack from your modems version. The erase of this section is protected. Check the modem version in Settings->About. It'll either be 3.12(1.0) or 3.14(1.0.1 and 1.0.2). You need the ramdisk which cooresponds to your version. Then go into "/usr/local/standalone/firmware" and get the ICE*.fls file. Extract 0x1a4-0x9a4 and save it in a file called secpack and place it in the same directory as the ieraser tool. Run ieraser. This should erase the modem firmware and leave you one more step on your way to unlocking.

POSTED BY GEORGE HOTZ AT 1:17 PM

25 COMMENTS:

S3bs said...

GoeHot... U r a genious... but i have a qustion... I'm from a foreign country... do you know if the iphone will work with sim cards from, for example, Argentina? ty... and waiting for more...

AUGUST 23, 2007 1:53 PM

Verner said...

It will work with any SIM card when it is unlocked.

AUGUST 23, 2007 2:00 PM

Jakob said...

Heya george, great that you keep up the steam!
I honestly thought you would stop this somewhat in the middle when you talked this morning (in my timezone) on

#iphone.unlock .
But I guess you're dedicated :D

Great work so far - I'm still impressed that you guys figured out how to bypass the NOR so you can patch it. Great achievement everybody!

Can't wait for the next and final part :) This will be 10% of the reason for me buying an iphone. The other 90% is split half and half between the iphone being a cool device that's very hackable and IF I can change the intelligent dictionary so I can be allowed to input danish words.

Thanks for what you and others have done so far!

AUGUST 23, 2007 2:36 PM

Christophe said...

So.. Can Apple easily put a stopper for this unlock by signing the file in tha main firmware where theese values are located???

AUGUST 23, 2007 2:37 PM

Christophe said...

Oh and great work Geohot :D

AUGUST 23, 2007 2:37 PM

jszeto said...

I agree too.. but would it make any different to pins on other parts of the same trace? e.g the bottom part!

AUGUST 23, 2007 8:30 PM

Antonio said...

Hi George, congrats. I have some doubt's about the hex dump you did on step 7 to generate the secpack file and in the step 8, did you use DD to export that ranges?

AUGUST 23, 2007 11:16 PM

lesterine said...

is this compiled for ssh or cmd in windows? or is this intel mac only file?

AUGUST 24, 2007 3:31 AM

Dorian said...

I can't believe it. Why the hell are you going to college when you could have made a fortune on the unlock? You said you didn't want people making money off of this. Are you knocking futs? There's maybe 10 or 20 people that can do what you did. Everyone else is going to buy it. Are you an IDIOT SAVANT?

AUGUST 24, 2007 1:54 PM

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

NYC said...

Could you be sue by the Apple and AT&T company for unlocking this phone or for publishing how go by on doing so. Do you need a partner to start a iphone unlocking business.

AUGUST 24, 2007 2:29 PM

Virginia said...

HOTZ, YOU CERTAINLY PICKED THE RIGHT PROFESSION TO GO INTO. THE HUMAN BRAIN HAS SOOOO MANY UN-HACKED AREAS. THE HUMAN RACE IS CERTAINLY BLESSED BY YOU AND OTHERS LIKE YOU.

I HAVE ALPHA 1 ANTITRYPSIN DEFICIENCY (HEREDITARY EMPHYSEMA). I RECEIVED A Z GENE FROM EACH OF MY PARENTS (RARE). ONE PROTECTS THE LUNGS, ONE ATTACKS THEM.

I'M ON THE WAITING LIST FOR A LUNG TRANSPLANT, BUT I'M A SMALL PERSON 5' 1", NOT TO MANY SMALL LUNGS DONATED. THEY HAVE TO FIT, THEY CAN'T CUT THEM DOWN, HA HA. THE AVERAGE WAIT ON THE LIST IS 6 MONTHS IN WASHINGTON, I'M GOING ON 2 YEARS.

WHILE YOUR HACKING INTO THE HUMAN BRAIN FIND THAT SECOND Z GENE AND SEE IF YOU CAN ALTER OR MAKE IT DESTROY ITSELF.

A THOUGHT TO PUT IN THE BACK OF YOUR MIND ON YOUR

A THOUGHT TO PUT IN THE BACK OF YOUR MIND ON YOUR JOURNEY THROUGH LIFE. MAY IT BE A GOOD ONE!!!

VIRGINIA

AUGUST 24, 2007 2:40 PM

Mike said...

Genius kid! Good onya my friend and thanks.
Mike
Firefighter Blog

AUGUST 24, 2007 3:59 PM

None said...

I have a question that should interest everyone here. What is the probability, do you think, that Apple and/or AT&T wil disable the unlocking method our Collegian friend?

marshall

AUGUST 24, 2007 5:09 PM

mAtNicK_@@_!!! said...

estou interessado em saber mais, favor responder
matheus_brito@hotmail.com
brasil.

AUGUST 24, 2007 5:39 PM

mAtNicK_@@_!!! said...

interessado em informatica, celular, e coisa e tal entre em contato matheus_brito@hotmail.com

AUGUST 24, 2007 5:42 PM

patriot1964 said...

How do you cut and paste all those computer words in?

AUGUST 24, 2007 9:06 PM

thatshyguy said...

where do you pu the sim card at in the iphone?

AUGUST 24, 2007 10:05 PM

Clay said...

Congrats on discovering what Apple and AT&T "Your

Congrats on discovering what Apple and AT&T "Your World...Monopolized" wanted so badly to keep secret: the iPhone lock!!!

But why should I pay you or any other hackers for unlocked iPhones???

You don't think that now the jig's up, Apple (who surely has some retentive iPhone rights of product) will now offer iPhone services to OTHER celluar providers???? Heh....to save that Steve Job ass from a monopoly suit (and you can bet one's in the oven a-cookin'), Apple will be all too glad to share the iPhone!!!!

Nice job, George!! Stay in school and bone up on that Engineering degree; a mind like yours will offer the Planet some pretty cool whiz-bang stuff!!!

AUGUST 24, 2007 11:15 PM

jamiev said...

Has apple offered you a job yet? genius !!! Nice work

AUGUST 25, 2007 12:40 AM

Spencer said...

will it work on Verizon

AUGUST 25, 2007 10:53 AM

Marc Sterling said...

May the souls of hackers and open source freaks be with you forever. Thank you for your amazing time and energy. You have done a huge service to bringing technology back to the people and away from wall street.

AUGUST 25, 2007 10:59 AM

Lorin said...

Small correction. That second group of addresses should instead be "0xA0040030 0xA004A5A0 0xA0055C58 0xA0057370". (Last two are different, the 4s should be 5s.)

AUGUST 25, 2007 1:33 PM

Preet said...

Dude you are genius. I am interested in finding out what all

resources did you tap in to get to know all the intricate details about hardware and software? Is it documented somewhere or was it mostly tial and error?

AUGUST 25, 2007 10:43 PM

Behzad said...

how do i go into /usr/local/standalone/firmwareusing ssh??? second how do i find bbupdater and where do i have to upload it so that i could run it

AUGUST 26, 2007 2:48 AM