FINDING JTAG ON THE IPHONE

THURSDAY, AUGUST 23, 2007

The Phone is for sale

eBay Auction

This is the phone that was unlocked live here this morning. It includes the phone, the worlds first serial dock, and the official unlock switch from the blog.

As a note, if you are only bidding on this to get an unlocked iPhone, don't. There are much cheaper and easier ways to get one. This is a piece of cell phone history. I have no intention of ever starting an unlocking service.

I'm sure these most recent bids are fake. I have a confirmed offer of $25,000 and an unconfirmed offer of $100,000. If you are willing to buy it for more, please post your phone number+email address+what you'd pay in a blog comment and I will contact you

POSTED BY GEORGE HOTZ AT 8:32 PM 312 COMMENTS

BLOG ARCHIVE

▼ 2007 (87)

▼ August (69)

The Phone is for sale

The Energy it took...

Postmortem

Step 10: The Last One

Step 9

Step 8

Step 7

Think of how pretty it'll be...

A Little Motivation

Step 6

Step 5

Step 4

Zoomed In Step 3

My Finished Step 3

Step 3

Step 2

SUNDAY, JULY 29, 2007

iPhone in hand, ready to begin...

Thanks to jpetrie, who donated an iPhone to the cause, I have an iPhone to take apart. I will be posting to this blog as I take it apart and discover things.

POSTED BY GEORGE HOTZ AT 11:34 PM

SUNDAY, JULY 29, 2007

My Workspace

POSTED BY GEORGE HOTZ AT 11:56 PM

MONDAY, JULY 30, 2007

Guitar Picks make great case opener tools

POSTED BY GEORGE HOTZ AT 1:03 AM

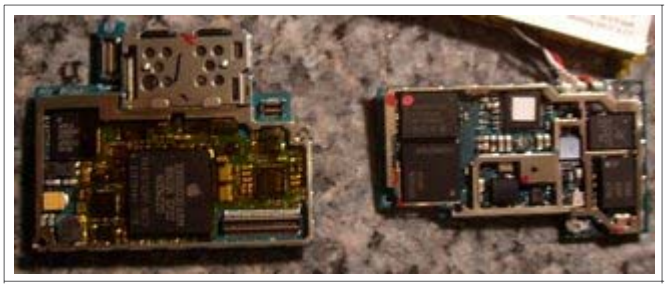
MONDAY, JULY 30, 2007

Getting there

POSTED BY GEORGE HOTZ AT 1:27 AM

MONDAY, JULY 30, 2007

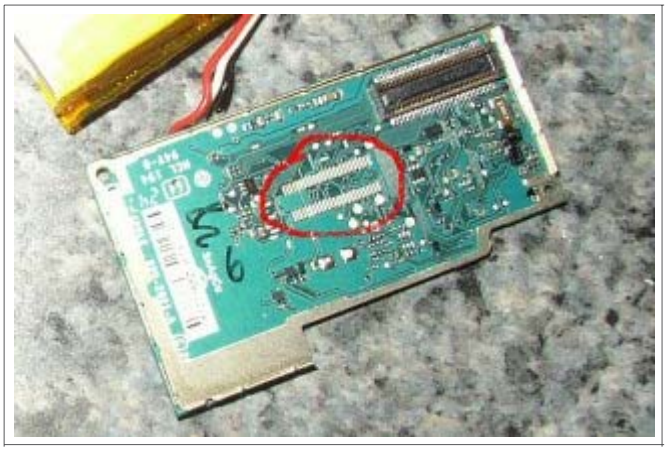
Wow this iPhone is full of chips too



POSTED BY GEORGE HOTZ AT 1:53 AM

MONDAY, JULY 30, 2007

Hmm...



I'd bet JTAG is on here, I am going to start seeing where these pads correspond to. I'm thinking JTAG is also somewhere more accessible.

POSTED BY GEORGE HOTZ AT 1:57 AM

MONDAY, JULY 30, 2007

iPhone battery extender

POSTED BY GEORGE HOTZ AT 2:49 AM

MONDAY, JULY 30, 2007

Well I guess I really didn't break it...

POSTED BY GEORGE HOTZ AT 3:19 AM

MONDAY, JULY 30, 2007

A theory

I'd bet that apple has a way to power up the baseband board without it being connected to the main board. I'd like to see what the main header contains.

That 52 pin unpopulated connector could be one of two things. Either a debug connector that apple used while troubleshooting the baseband, or a connector for another revision of the iPhone main board. I am leaning toward the latter. I'd think that JTAG is actually present on both connectors, and that Apple accesses it through something like the camera port. The camera only appears to use half the pins on the connector. So once I get a multimeter that doesn't suck, which will probably be tomorrow, I will test for continuity between the camera header and the board interconnect header. I'd bet that there are a few pins in common, and those are JTAG.

POSTED BY GEORGE HOTZ AT 3:39 AM

---

1 COMMENTS:

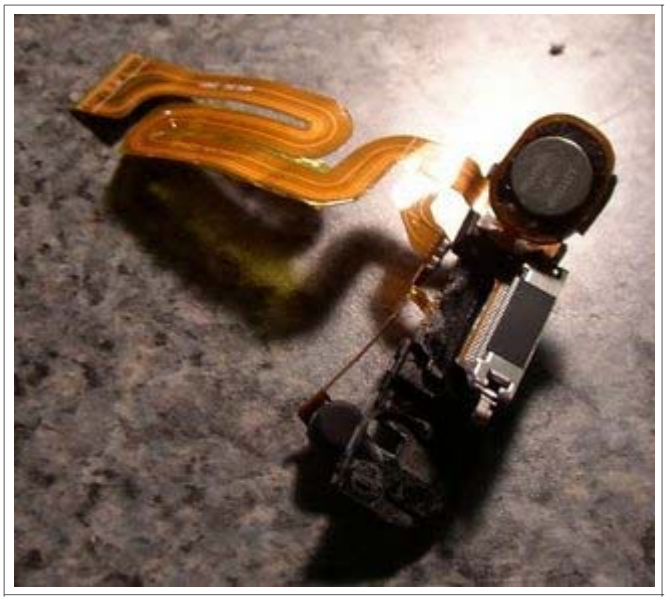
tom said...

While you're poking around in there, it would be interesting to see if there's video output somewhere.

JULY 30, 2007 4:17 AM

MONDAY, JULY 30, 2007

Dock Connector removed



POSTED BY GEORGE HOTZ AT 2:54 PM

MONDAY, JULY 30, 2007

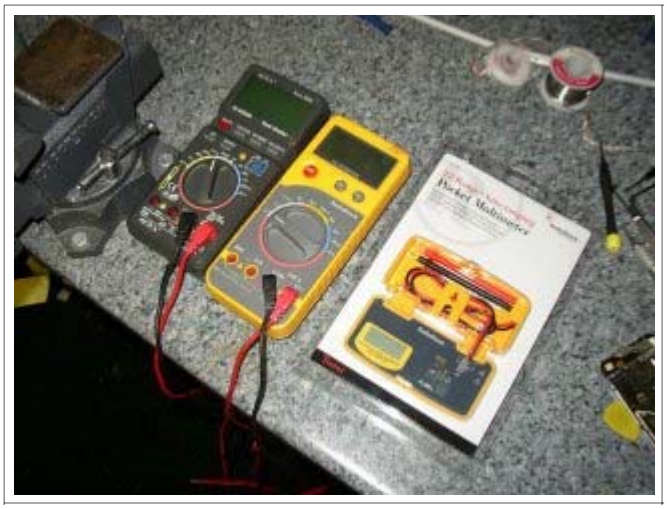
Wow it still powers up...

The only connectors still connected are the two to the screen and the top button connector.

POSTED BY GEORGE HOTZ AT 3:05 PM

MONDAY, JULY 30, 2007

Stupid Multimeters

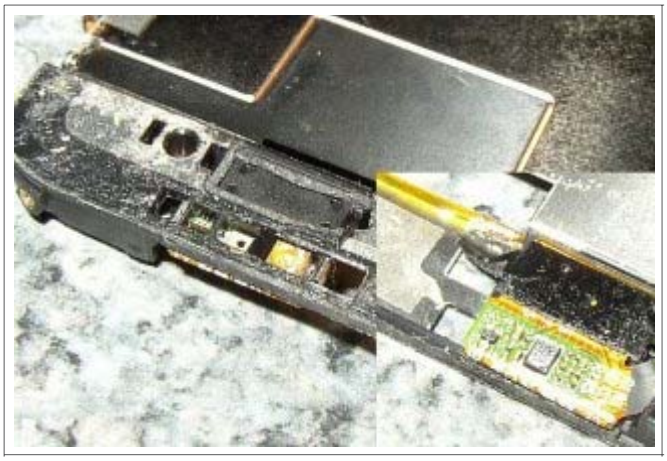


The $100 multimeters can't beep right away with the continuity check. This $30 one can.

POSTED BY GEORGE HOTZ AT 3:30 PM

MONDAY, JULY 30, 2007

Proximity Sensor



This looks a lot like IR hardware...

POSTED BY GEORGE HOTZ AT 3:40 PM

---

1 COMMENTS:

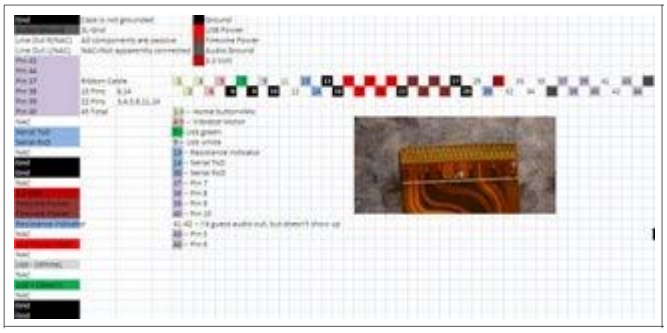
Ronald said...

I believe that the proximity sensor IS an infrared sensor. The iPhone page that explains the sensors says it emits infrared light.
http://www.apple.com/iphone/technology/

JULY 31, 2007 1:45 AM

MONDAY, JULY 30, 2007

The Dock Connector



A few notes:
The firewire power is present, but not the data
The old video pins/line in pins are connected to the main board(JTAG maybe)
The line out pins don't make a direction connection from the board to the conn
A bunch of pins on the conn have traces, but idk where they are connected

POSTED BY GEORGE HOTZ AT 6:40 PM

MONDAY, JULY 30, 2007

When does an iPhone stop being an iPhone...

This still connects via USB.

POSTED BY GEORGE HOTZ AT 11:42 PM

TUESDAY, JULY 31, 2007

"Permission Denied"

I am thinking that the only thing that keeps the iBoot "Permission Denied" errors around is the lack of a proper resistance on the accessory indicator pin. But I'd bet the resistance is very specific. bluetang found the "This accessory is not made to work with iPhone" string in IAP.framework's Framework.strings file, so I think reversing the program that calls this would be a good idea. Find the resistance ranges that the iPhone likes.

POSTED BY GEORGE HOTZ AT 3:14 AM

---

2 COMMENTS:

Brazuca said...

don't know if you saw this, but it has common resistance values for the iPod dock connector. Maybe something (or someone) or use can be found there.

http://www.ipodlinux.org/Dock_Connector

quote:

Pin 21 connected to ground via a resistor. Different resistances indicate which accessory is connected. Known resistances/functions (ohms) are as follows:
1 kΩ - iPod docking station, iPod beeps when connected
10 kΩ - Takes my iPod into photo import mode
500 kΩ - vava uses this for his serial-via-dock experiments. Used in Dension Ice Link Plus car interface
1 MΩ - Belkin auto adaptor, iPod shuts down automatically when power disconnected

JULY 31, 2007 9:48 AM

mickangel said...

Food for thought, N95 unlock hack:
http://www.ipmart-forum.com/showthread.php?p=1449507

JULY 31, 2007 1:55 PM

TUESDAY, JULY 31, 2007

Priorities...

JTAG: This is a sure unlock, but it is hard to find. I don't think it is on the dock connector, instead I think pins 7-10 are the network port. I am going to spend the reset of the day trying to power up of baseband board standalone.

AH5DD: This is the "Apple H5 Debug Dock" H5 is low level serial over bluetooth protocol. See here for the spec. The iPhone is believed to output a very low level signal that can be picked up and connected too. I've heard that a patch exists for BlueZ to implement H5. I'm not sure what you would see if you did establish a connection, but "debug" is always cool.

Baseband Bootloader: The baseband bootloader has an interactive mode which is used to download the firmware/eeprom. It also supports reading of the data. This could lead to a memory dump, which would make the firmware *so* much easier to follow.

I want to keep everyone updated with the fronts the unlock is being tackled from, and if I ever post something like 'we are working on "several fronts" for an unlock' and leave it at that, please slap me :-)

POSTED BY GEORGE HOTZ AT 6:03 PM

---

2 COMMENTS:

Jason said...

All I can say is you awe me. I truly wish I had your skills and I VERY MUCH thank you for your efforts. I am an American abroad in Argentina anxiously awaiting my newly ordered 8GB iPhone and I have every confidence that when it arrives in 4 weeks I will be good to go!!! Fily unlocked ... and with a terminal app!!!! Thank you hackers of the world!!!!!

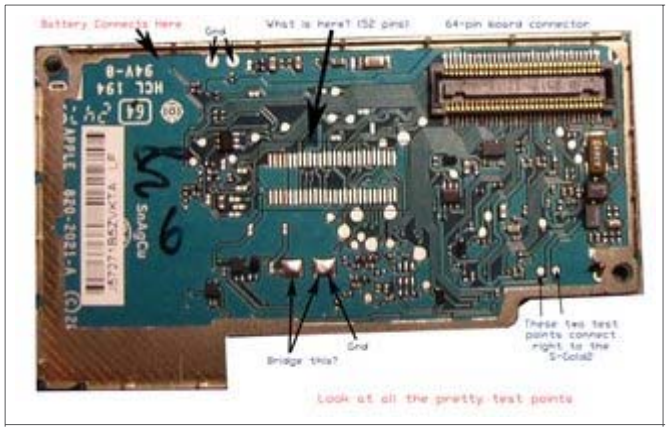
JULY 31, 2007 11:19 PM

mickangel said...

Well done. I appreciate you keeping your updates transparent and open. Please keep up the great work.

TUESDAY, JULY 31, 2007

Baseband Board Backside



POSTED BY GEORGE HOTZ AT 8:07 PM

WEDNESDAY, AUGUST 1, 2007

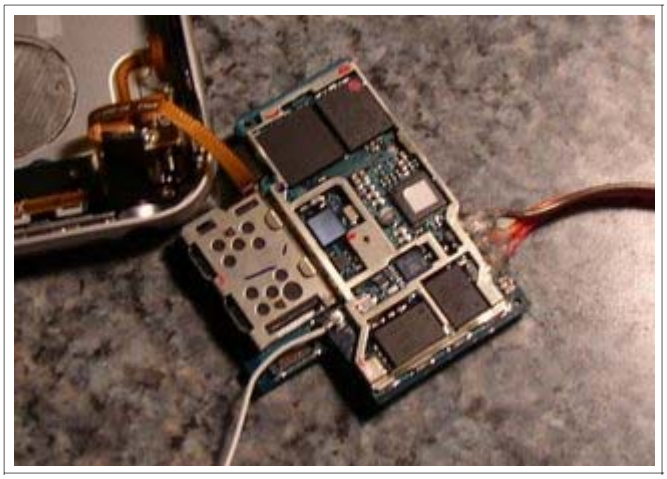
The update...

The baseband firmware was updated from 03.12.06 to 03.14.08 The bootloaders aren't included in seperate files anymore, and there aren't three of them. The eep files have very minor differences. And imeisv and bbupdater were changed a little; I haven't loaded them in IDA, but the changes are probably very minor. For unlocking purposes, ignoring the update is probably the best option.

POSTED BY GEORGE HOTZ AT 12:35 AM

WEDNESDAY, AUGUST 1, 2007

I can SSH into this...

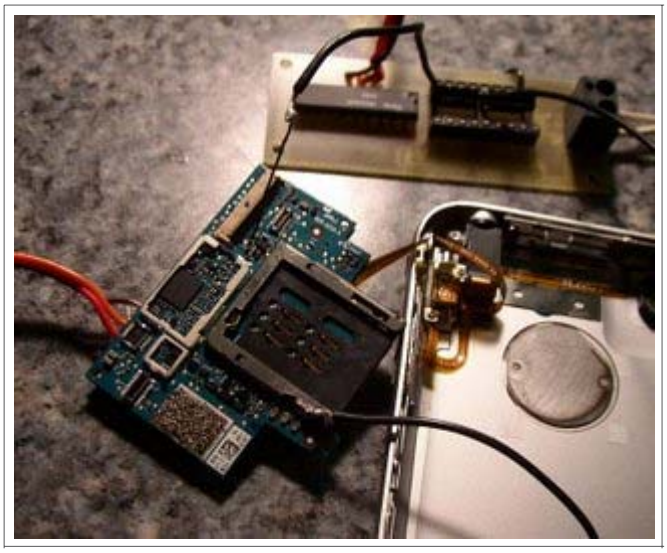


All you need is the battery, the WiFi antenna, and the power button.

POSTED BY GEORGE HOTZ AT 1:26 AM

WEDNESDAY, AUGUST 1, 2007

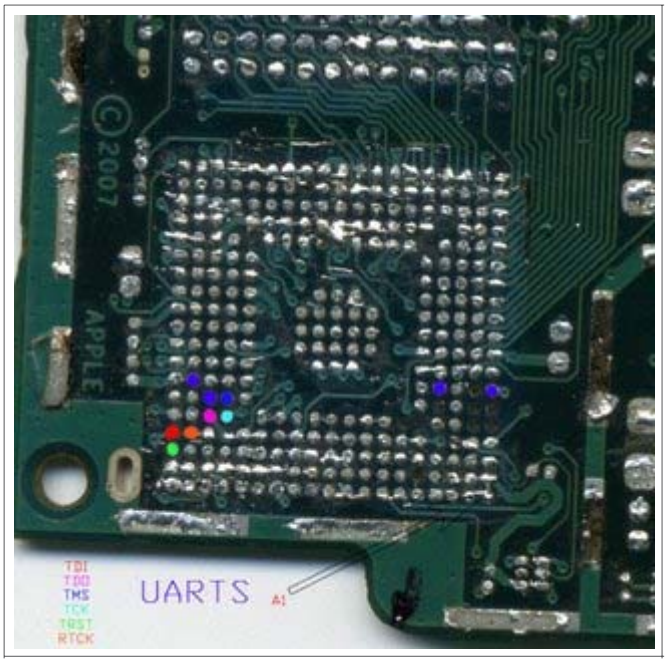
Serial with a test point



POSTED BY GEORGE HOTZ AT 5:53 AM

WEDNESDAY, AUGUST 1, 2007

S-Gold2 JTAG confirmed broken out



Thanks to Nick Chernyy we got scans of iPhone bare boards. I see vias for TDI, TDO, and TCK, and I can't see a reason Apple would do that unless JTAG was accessible somewhere. I wish I had these boards to probe.

POSTED BY GEORGE HOTZ AT 10:14 PM

THURSDAY, AUGUST 2, 2007

Last Resort

Unfortunely the boards in the pictures below have been destroyed. So probing them is out of the question. The traces in the pictures are very hard to trace anywhere because this board has many layers and blind vias. So here is what has to be done, the S-Gold2 has to be removed from the board. Once this is done I will have full access to the pins of the chip; and I know the pinouts. In the previous post I showed the location of the pins to probe. The chips are sealed to the board and don't have any place to stick a small wire in. So the only option is to remove the chip.

It makes me really sad to wreck an iPhone like this, but there are two plus sides. One, only the communications board will be touched. And a replacement is only $150. Two, if I do this really carefully I could get a new S-Gold2 and replace it. Possibly the old one could even be reballed.

The information we will get from this is, I feel, worth the sacrifice. If this goes well, we will know the location of JTAG within a few hours. The donation pot has reached $509, and I'll put the rest in to get a 4GB iPhone tomorrow. Because we need an iPhone to actually do the JTAG into. Now more then ever, we need donations. We still need to buy a JTAG adapter. My paypal address is geohot@gmail.com

POSTED BY GEORGE HOTZ AT 1:11 AM

THURSDAY, AUGUST 2, 2007

It's go time...

First of all, thanks so much for all your donations, it's you that make this possible. Here is how things are going to go down. It's 7 AM now, and I have a linux box and a homebrew JTAG adapter. I leave here at 8:15 and pick up bagels. I like bagels. Then it's off to these guys to see if they can remove the S-Gold2 from the communications board. If not, it's over to Home Depot for a heat gun, seeing as mine sparked and died last night. Then I'll head over to the Apple store and pick up an iPhone. After probing the contacts, I'll get the location of JTAG on the board and connect up my adapter to the new phone. Hopefully it'll connect, and I can download and modify the full contents of the BB NOR flash+ram!!!

POSTED BY GEORGE HOTZ AT 6:45 AM

---

1 COMMENTS:

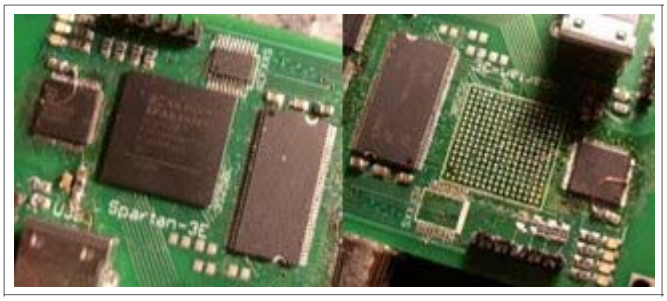
deeda Inc. said...

1-20-9-6 @ 4-5-5-4-1 . 3-15-13

AUGUST 24, 2007 3:18 PM

THURSDAY, AUGUST 2, 2007

BGA Removal

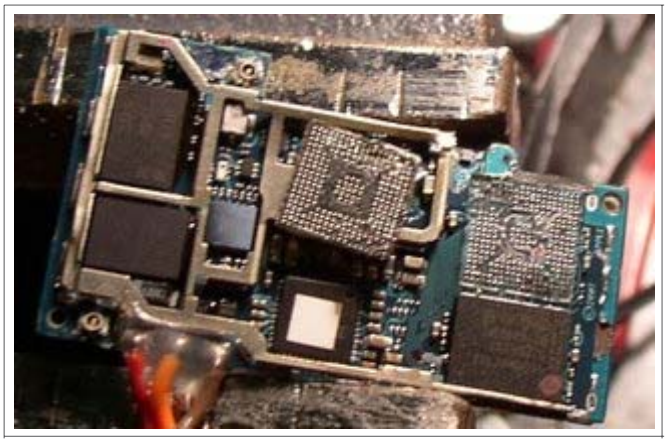


The place couldn't do it so I bought a heat gun. 254/256 isn't bad

POSTED BY GEORGE HOTZ AT 10:13 AM

THURSDAY, AUGUST 2, 2007

It looks bad, but it's good

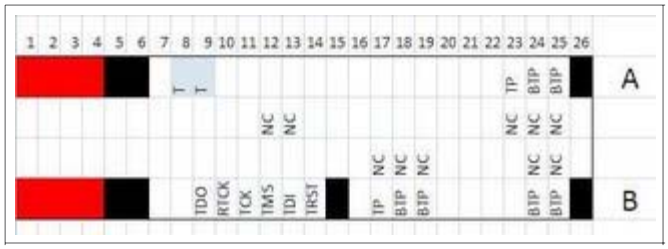


The pads were smaller than I imagined. All the JTAG pads are intact and ready for tracing.

POSTED BY GEORGE HOTZ AT 10:28 AM

THURSDAY, AUGUST 2, 2007

WE FOUND BASEBAND JTAG



This is the 52 pin connector as viewed with the square corner of the board in the upper left. This is really awesome...but we have a casualty. An iPhone died in the making of this picture. RIP

POSTED BY GEORGE HOTZ AT 11:27 AM

---

4 COMMENTS:

TheVoodooInfo said...

Following this closely!! I hoped that "the dev team" kicking you out wouldn't kill your phenomenal contributions to this "project"... Much props!

AUGUST 2, 2007 2:04 PM

Manjit said...

I too have been following your and DEV caps work with great interest. Its shame a load of politics broke the camp, but you sure have your spirits up dude and are doing a great job. Wishin you success all the way!! Seems very close now.

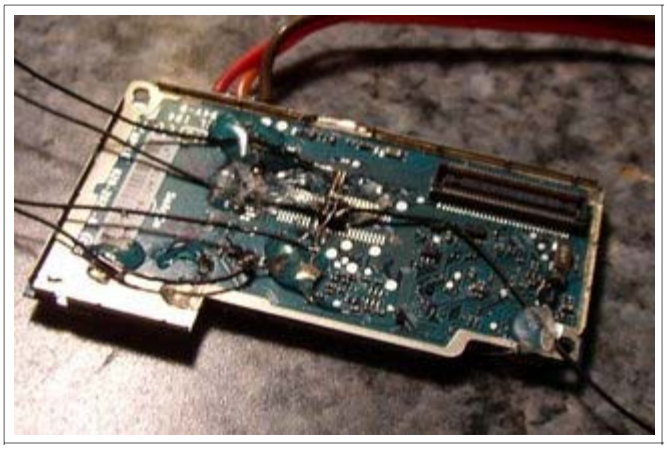
AUGUST 2, 2007 4:23 PM

Victor said...

This sounds greate, I hope you find the NCK or what else is needed to unlock the iPhone. I hope it will be a software solution so we could run a software on our mac or pc and connect iPhone and type unlock or something like that. Thanks for all good work and good luck.

THURSDAY, AUGUST 2, 2007

Hardest Soldering I have ever done



Those pads are very very very small. It looks like crap, but electrically its good.

POSTED BY GEORGE HOTZ AT 9:30 PM

---

1 COMMENTS:

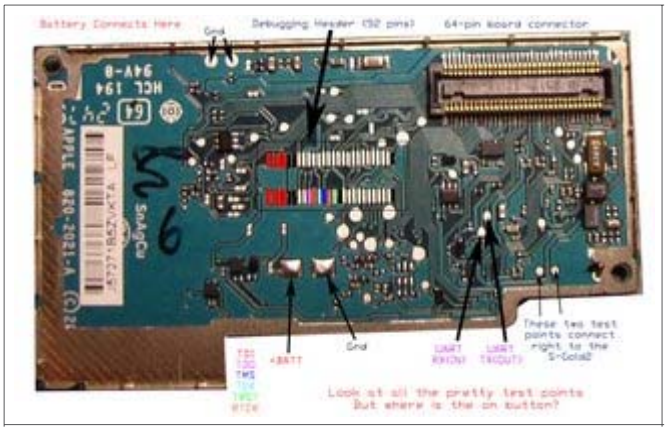
iphonefan said...

amazing stuff. keep up the good work, george

AUGUST 3, 2007 4:15 AM

THURSDAY, AUGUST 2, 2007

Updated...UART found



All the JTAG pins are soldered, but the only problem is we don't know how to turn the board on.

POSTED BY GEORGE HOTZ AT 11:16 PM

---

5 COMMENTS:

Diet said...

Great work indeed! But probably you'll need both of the boards connected if you want to switch on the phone ...

AUGUST 3, 2007 2:38 AM

Philipp said...

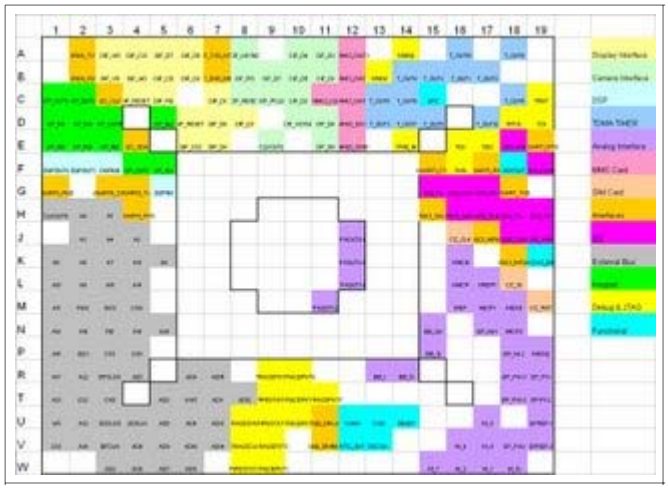
Oh my god, I have no idea what you are doing. lol I don't understand any of it but it looks cool. Maybe at some point you can give us an update in plain english how all of this might lead to the unlocking of the iPhone. :-)

Good work!

AUGUST 3, 2007 3:55 AM

FRIDAY, AUGUST 3, 2007

Where we stand...

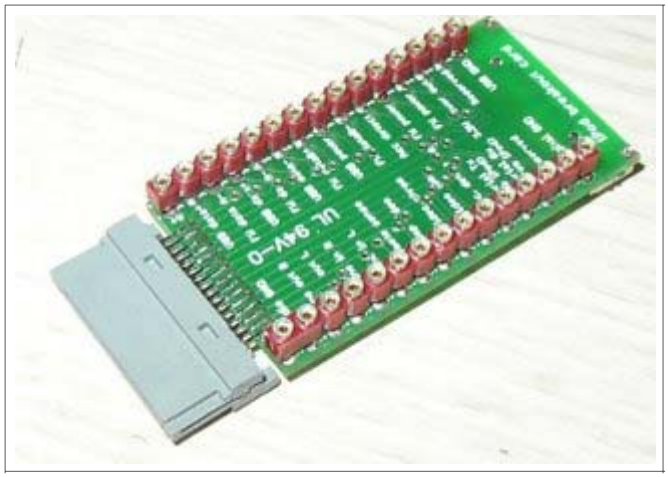


So we still haven't powered up the board. I have heard two suggestions over and over throughout the day, so I will address them. One, why can't you put the boards back together? I could but I would have to desolder what I did for JTAG. I still think it shouldn't be too hard to find the "on button" We are still looking for the connectors, so we can probe the 64-pin header. The other suggestion probing the interboard connector; get me a connector first. I made this pinout sheet because I like pretty colored diagrams of stuff. And Wind River, expect a call tomorrow. That's what you get for mentioning a 52-pin debug header without providing pinouts :)

POSTED BY GEORGE HOTZ AT 5:06 AM

FRIDAY, AUGUST 3, 2007

Elusive Power Button



We still haven't found the power button, because we still don't have a datasheet for the PMB6812. On the plus side, my dock breakout board finally came in the mail today, so tonight I will probe at it. I'm pretty sure there is no JTAG on the dock, but pins 7-10 are, I think, an ethernet port. That'll be cool to find.

POSTED BY GEORGE HOTZ AT 4:58 PM

---

2 COMMENTS:

Feraldax said...

Maybe that helps:

http://www.infineon.com/dgdl/PMB6811_Product+Brief_1003.p

stay cool

AUGUST 3, 2007 6:27 PM

steven said...

If you still need to know the internal traces, I have access to a hi-res X-ray machine. We use it at work to check FBGAs and other bottom only terminated devices for good solder. I think it would work great to get a better look at the internals of the PCB. Let me know...

AUGUST 3, 2007 11:41 PM

SATURDAY, AUGUST 4, 2007

So Modular...

We aren't haven't any luck finding the power button for the baseband. We will eventually get the datasheet, but until then... When I first soldered the JTAG I wasn't aware of how difficult it was going to be. I rushed into in and didn't do such a clean job. It will work, but I couldn't put the boards back together with it. So I took apart my personal iPhone and decided to JTAG it. I desoldered a power connector off the dead iPhones logic board. Desoldering connectors is really really hard, because it is so easy to melt the plastic. But I got it and soldered it to the JTAG header. Now, with that connector in place, the boards will snap together ok. So the plan is to snap the boards together, power up the baseband, then disconnect the boards. I believe the comm board will stay powered on, so then I just connect the JTAG connector and JTAG in...

POSTED BY GEORGE HOTZ AT 3:55 AM

---

1 COMMENTS:

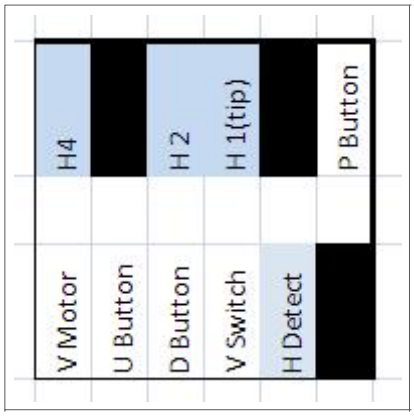
Diet said...

I'd suggest another way to connect the JTAG wires: use magnet wire to do the connections to the pads, secure the magnet wire with adhesive tape instead of hot glue and then you can snap the two boards together while the wires are connected and are accessible from outside.

AUGUST 4, 2007 4:14 PM

SATURDAY, AUGUST 4, 2007

Headphone+Switch Connector



Figured since I was butchering this anyway, I should get the pinouts.

POSTED BY GEORGE HOTZ AT 5:32 AM

SATURDAY, AUGUST 4, 2007

Cable Done

The cable is done. Electrically perfect except that TRST short to two tracepkts on the other side. I will fix this if needed, but I don't think it'll matter. Also, no hot glue, I discovered the wonders of blue tape :)

POSTED BY GEORGE HOTZ AT 6:21 AM

SATURDAY, AUGUST 4, 2007

Doesn't stay powered up

The comm board doesn't stay powered up when you disconnect it from the main board. This is rather sad, meaning we still need to find the on button. The above trace is of RX, TX, and B1. Remember that RX comes from the logic board. I still think B1 looks like a power on signal. I also found that TX goes low on a baseband reset through the AppleBaseband kext, but that TX/RX don't appear to be tty.baseband. Which is weird, but maybe they do the baseband trace.

POSTED BY GEORGE HOTZ AT 7:37 AM

---

3 COMMENTS:

Keanu said...

Hi,

I have found that PMB6812 has I2C interface, so maybe this is used for power up ?

AUGUST 4, 2007 12:33 PM

Brazuca said...

keanu, join us at #iphone.unlock (in us.undernet.org)

AUGUST 4, 2007 1:35 PM

Henning said...

George et al. you are so great! Thank you so much for all your efforts!
Greetings from Vienna, Austria!

AUGUST 4, 2007 3:32 PM

SATURDAY, AUGUST 4, 2007

Where we are...

First I got a few requests to explain in plain english what the purpose of this is. I will try. Ok, JTAG is the lowest level debugging. JTAG is an interface, availible to almost every processor, which supports simple commands like "PEEK" and "POKE" If you remember from the Apple II days, these commands will raw read and write to memory. Now I've also gotten a few question from people concerned that they can't do the JTAG mod themselves. Hopefully, you won't have to. The idea is to get dumps from my chip and find a software exploit we can use to unlock the phone. So you won't have to deal with JTAG at all, but you will get an unlocked phone.
If you want to help find the datasheet, the part number is PMB6812. The 2 page product brief is not the datasheet, and doesn't contain the information we need. The real datasheet will contain pinouts and be over 10 pages.
Also does anyone know about martech.pl These guys seem to unlock S-Gold2 based phones with two test points. What are these test points? What do they send to them?

POSTED BY GEORGE HOTZ AT 4:14 PM

7 COMMENTS:

Fernando said...

This post has been removed by the author.
AUGUST 4, 2007 7:22 PM

Fernando said...

Nevermind, it's the product brief. Sorry.

AUGUST 4, 2007 7:28 PM

Michael said...

Are you sure its PMB6812? This looks like a power management chip. http://www.neonseven.com/PDF/N711.PDF has a prototype cell kit using this chip which includes a lot of info

AUGUST 4, 2007 8:05 PM

SUNDAY, AUGUST 5, 2007

NOR Flash Dumped by dev team

Nice job on the NOR flash dump. I seriously mean this, I couldn't figure out how to do this. But since you just posted your tool without any explanation, I'll try to fill everyone in. The dev team has succeeding in dumping the NOR flash by using the bootloaders interactive mode. This contains the bootloader, the main code, and the eeprom. So why do we still need JTAG? A NOR dump is very different from a running RAM dump which JTAG can do. I have no idea where anything is stored in the NOR flash. I couldn't find the IMEI in the dump, so I am assuming it's encrypted in some way, probably the same way the NCK is. With JTAG we can get a running RAM dump and extract the NCK while it is being checked. JTAG is like a debugger. We can set registers then run the code to fetch the NCK. Simply by reading locations in memory we can get it. The NOR flash obfuscates it in some way. I may be totally wrong, but I don't want to invest time doing work that the dev team has already done. Also, using this dump method, it will never be possible to get a running ram dump, because the dumper runs using the bootloader; before the main code is executed. Dev team, can't you just make your source and findings public?

POSTED BY GEORGE HOTZ AT 4:49 AM

---

2 COMMENTS:

Fernando said...

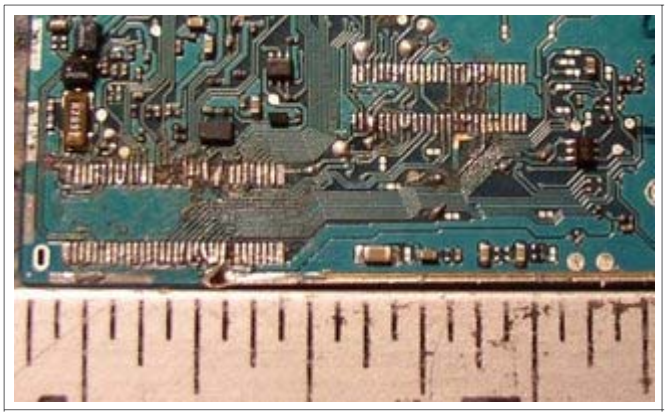
I guess not. The "Dev Team" wants all the glory for themselves. I think I wouldn't be surprised if they asked for a "donation" in exchange for the true unlock...

You've done a great job. Keep it up. I'm still coming here everyday to see how you're doing and if you need any help.

AUGUST 5, 2007 7:53 PM

SUNDAY, AUGUST 5, 2007

Connector Size



POSTED BY GEORGE HOTZ AT 6:27 AM

SUNDAY, AUGUST 5, 2007

This is taking forever...

It is really hard to get tbe jtag soldered while still retaining the ability to put the boards back together. Hopefully we will be getting the datasheet soon, so we can start looking for the power button again. The power up isn't simple, and because of that the best solution is to just JTAG with the boards still connected. I thought that sounded rigged at first but the "power button" is really hard to push.
The easiest way to do the soldering would be to find a cable like this and soldered that right the the connector. But the pitch of the iPhone is really weird, I keep getting like .383mm If I had a .4mm ribbon cable I could probably use that. When I get home, I will make an eagle cad file of a flex breakout board. spoonet said he may be able to have this laser cut. Also I will try to make the flex board myself.

POSTED BY GEORGE HOTZ AT 7:48 PM

---

2 COMMENTS:

Diet said...

As written earlier: I'd suggest to use magnet wire ("kupferlackdraht") soldered to the JTAG pads and fix it using adhesive tape. With that it should be no problem to snap the boards together while the wires are connected. Sure, it's a bit damageable but I think you don't need moving it around too much.
Good luck!

AUGUST 6, 2007 2:16 AM

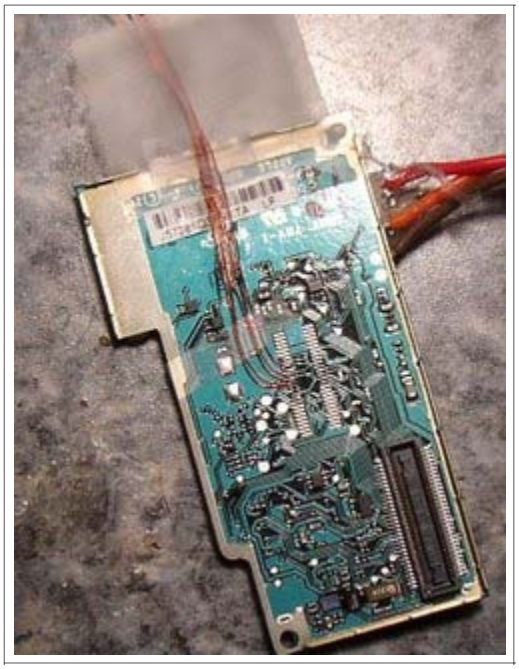
Nicolas said...

You are doing an amazing Job! Im checking you blog daily, but i dont understand very much what you are doing.

I think the NOR Flash is available now at de Dev Wiki page. Maybe im wrong, but there is actually somtheing for download a their page:

MONDAY, AUGUST 6, 2007

Soldered



I knew if anyone could do this soldering, it would be my ex-mentor and friend Joe Barbetta. I brought the board down to his shop this morning, and under a microscope with some very fine gauge magnet wire, he soldered it. Thanks.

POSTED BY GEORGE HOTZ AT 12:41 PM

---

5 COMMENTS:

Diet said...

looks *very* good - just as I'd have done it! hopefully the JTAG debugging sessions can start soon now :) you're doing a really great job - congrats!

AUGUST 6, 2007 1:05 PM

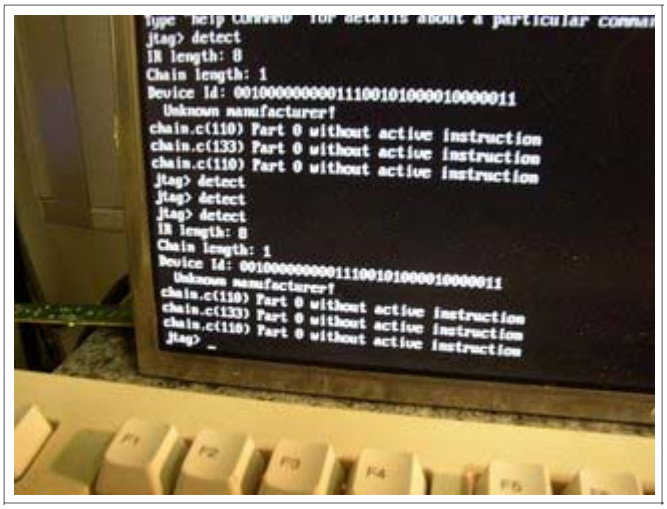
Steve said...

I haven't a clue what your doing other than trying to unlock the iphone. Anyway just wanted to give my support and say keep up the good work it all looks great. I also appreciate the regular updates whether they make sense or not, it gives the impression that somebody is at least trying. Thankyou for your efforts. Steve

AUGUST 6, 2007 1:51 PM

MONDAY, AUGUST 6, 2007

THE CHIPID HAS BEEN READ



The chipid has been read, so that means the JTAG hardware is working. The first half of the battle is over. I used OpenWinCE to connect, but it doesn't support this chip yet. So now we have to write software for JTAGing ARM926. But we know that the hardware is working!!!

POSTED BY GEORGE HOTZ AT 1:54 PM

---

6 COMMENTS:

Fernando said...

That is pretty great! I really don't know how you're going to do the software, but if you need any help just post it and I'm sure someone who is able to, will come forward. I personally would, but I am not certain what kind of programming is involved.

AUGUST 6, 2007 3:01 PM

Oleg said...

Hello George! Great work... Congratulations. About ARM JTAG software: take a look at Wind River Workbench.. I think you will be winner with this thing. (I've just seen it in eDonkey network). So you easily can get it.. Cheer, Oleg

AUGUST 6, 2007 3:51 PM

MONDAY, AUGUST 6, 2007

You have JTAG, where is the unlock?

Here is the idea once we do get JTAG, and I'll explain why we don't have it later. The function that handles the CLCKing of PN clears two 16 byte blocks of memory. One has the user entered NCK copied into it. The other, I can only assume, has the real NCK. In that function, the real NCK is cleared from memory. So the idea is to put a breakpoint right before that clear, and read the contents of memory. JTAG should be able to do this, but the current software isn't working right. I know that all the hardware works, but for some reason the software will only connect when I set an Instruction Register length of 8. But all ARM9 processors should have an IR length of 4. The halt command isn't working, and that is the first step toward a gdb over jtag interface. So if you have any ideas about this, please tell me.

POSTED BY GEORGE HOTZ AT 11:47 PM

---

1 COMMENTS:

AT91 said...

Hi,

Check the 464709_DS.pdf, except the
ARM core you have DSP and MOVE cooprocessor.

One question - why is your JTAG pionout different then the actual wires you soldered ?

AUGUST 7, 2007 3:49 AM

TUESDAY, AUGUST 7, 2007

The BB board makes noise...

Well, I think the IR register length of 8 is okay. The JTAG is totally non standard. Infineon has modded the hell out of it. So we need one of three things, in order of goodness. One, S-Gold2 datasheet. Two, S-Gold2 jtag tools, but not the lauterbach ones. Three, another datasheet for an Infineon ARM9 chip with JTAG.

IR=Len of DR
00000000=510
00000001=510
00000010=510
00000011=510
00000100=32
00000101=32
00000110=1
00000111=1
rest are 1
00100010=1(MAKES SOUNDS)

POSTED BY GEORGE HOTZ AT 4:01 AM

TUESDAY, AUGUST 7, 2007

So Infineon JTAG is documented

HERE. And the lengths match what I found.

POSTED BY GEORGE HOTZ AT 4:11 AM

---

5 COMMENTS:

Diet said...

Great! Hopefully the security implementation mentioned on page 54 is not too bad ...

AUGUST 7, 2007 4:33 AM

Matthijs Thalen said...

This post has been removed by the author.
AUGUST 7, 2007 5:16 AM

Philipp said...

So, how close are we? :-) What does this mean to the overall scheme of things? :-)

AUGUST 7, 2007 5:53 AM

Assad said...

They maybe got some documentation ....

http://www.ifixit.com/iPhone-Parts/iPhone-Communications-Bo

AUGUST 7, 2007 8:06 AM

Fernando said...

Wow holy crap. This is amazing! You've done an amazing work! Keep it up!

AUGUST 7, 2007 1:50 PM

TUESDAY, AUGUST 7, 2007

Doesn't seem to be working

I wrote code to run the Cerberus commands as detailed in the doc, but they don't seem to work. Either the S-Gold2 doesn't support these commands, I overlooked something stupid, or the security features are set.

POSTED BY GEORGE HOTZ AT 7:30 PM

WEDNESDAY, AUGUST 8, 2007

JTAG Commands

0x00-0x07 Standard JTAG CMD's

0x10 Should be CCONF but acts like bypass(no 1)

0x22-0x23 noisemaker, randomly garbled data

0x2e 0xffff passes through, else 0x0000

0x54-0x55 always return 0

0xC0-0xCF Cerberus

Every other command behaves as a bypass

POSTED BY GEORGE HOTZ AT 2:50 AM

WEDNESDAY, AUGUST 8, 2007

We haven't hit security yet...

I'll start by saying JTAGing in is still a very viable option. My current understanding of security is this, it only stops *running* memory access. Pre-reset halted memory access should work fine anyway. If we hold the reset pin while setting jtag up it should work. This can be done in software by patching AppleBaseband. It's also very possible that it will work as is, and we just don't have the right commands. We know Infineon has make changes to Cerberus since that doc was written. So find the latest Cerberus doc...

POSTED BY GEORGE HOTZ AT 7:06 AM

WEDNESDAY, AUGUST 8, 2007

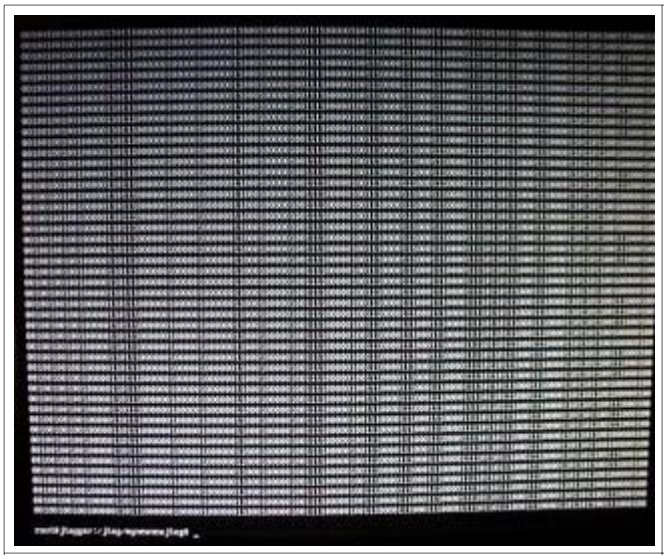
IO_SUPERVISOR

This command doesn't work, and it needs to work. Latest code is here. No further progress can be made on JTAG until we figure out why this command doesn't work. Read the docs here and here. We cannot do anything more until this works. I have tried a lot of things, and no luck. This isn't security, no security I've heard about would cause IO_SUPERVISOR to fail. It just keeps returning 1's and stays busy forever.

POSTED BY GEORGE HOTZ AT 6:58 PM

THURSDAY, AUGUST 9, 2007

New Angle



Cerberus isn't working, I'm stuck on that IO_SUPERVISOR command. So I figured I take a more basic look at jtag. JTAG has to implement two basic commands, EXTEST and SAMPLE/PRELOAD. EXTEST will load a register onto the I/O bus. SAMPLE/PRELOAD will read the IO bus and load that register. Now what good is raw access to the I/O pins. Well NOR flash is one on the simplest things to use; basically load the address bus, then pulse a pin to read, or load the address and data buses, and pulse a pin to write. So this should give us halted access to the NOR flash. With halted access, assuming we figure out how to patch out the sig checks, we could upload a modified firmware. Unfortunately we have no idea where any of these I/O pins correspond to. The register is 510 bits long. A datasheet for the S-Gold2 will tell us this. But it may be possible to determine with some clever reasoning.

POSTED BY GEORGE HOTZ AT 1:33 AM

THURSDAY, AUGUST 9, 2007

Not that way to the NOR

Although I am reading from the io pins themselves, the A* pins must not be included. There must be a controller for the NOR flash that this dump isn't accessing. These are dumps of the SAMPLE/PRELOAD command at 50ms intervals. They are online here.

POSTED BY GEORGE HOTZ AT 5:29 AM

---

2 COMMENTS:

Matthew said...

Not sure whether this might help but the recent JTAG connections I have been working on use secure JTAG.

The secure JTAG I am familiar with usually requires two keys. One of which may be a hash of the board-id/chip-id. Sorta like a user password scenario. The other is generated in some other fashion.

Using the correct keys then allows access to the standard JTAG commands.

AUGUST 9, 2007 10:09 AM

Brazuca said...

matthew, join the #iphone.unlock channel in us.undernet.org

Geohot is usually active (not sleeping) from the evening until the morning.

AUGUST 9, 2007 10:54 AM

THURSDAY, AUGUST 9, 2007

The drink of choice for leet hackers...

...who can't afford red bull.

POSTED BY GEORGE HOTZ AT 10:51 PM

---

2 COMMENTS:

MaxMalta said...

This post has been removed by the author.
AUGUST 10, 2007 12:53 AM

MaxMalta said...

Geohot, i found a Datasheet with 40 pages of pmb8876. Open this pdf and go to page 08. I hope that help we. Thanks, Max Malta, from Brazil.

Download it from my website:
http://www.max-systems.com/pmb8876.pdf

AUGUST 10, 2007 1:03 AM

FRIDAY, AUGUST 10, 2007

UARTs UARTs everywhere

It's getting hard to make progress on JTAG, so I decided to relook at the UARTs. I logic analyzed the UART we found on the test points eariler. It is /dev/tty.debug, and thats why it isn't used on startup. It is called UART0 by the S-Gold2. Therefore UART2 is /dev/tty.baseband But the chip only has 2 standard serial UARTs. I think UART2 is the USIF interface, but this is really just a guess. UART1 definitely doesn't connect to the logic board, because it is not on the connector. In fact I couldn't find it anywhere on the board. It may not be broken out. It's also weird that tty.debug only works for a little while after resetting the baseband. So therefore, AT+XSIO=2 shouldn't brick the phone. UART2 is the one you have to be careful of disabling.

POSTED BY GEORGE HOTZ AT 2:48 AM

FRIDAY, AUGUST 10, 2007

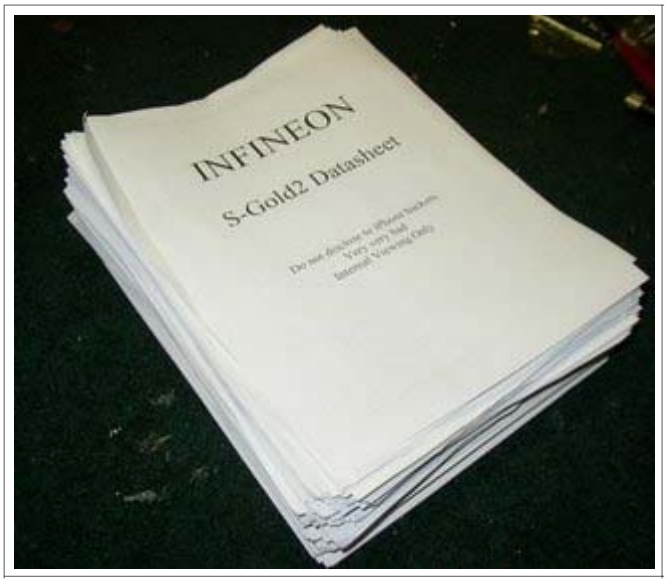
Trace Mode...Not even a hardware hack

Since we figured out which UARTs were which, I figured it was safe enough to enter trace mode. UART2=tty.baseband UART0=tty.debug So run AT+XSIO=2, reboot, set AT+TRACE=1, and minicom to /dev/tty.debug When I run AT I get
.P. ..SCC: T:0 C: ATSCC: T:0 R: OK
as a response.

POSTED BY GEORGE HOTZ AT 3:23 AM

FRIDAY, AUGUST 10, 2007

S-Gold2 Datasheet



I heard rumors that the full S-Gold2 datasheet was 1200 pages. So I went around my house and collected all the papers I could find, just to get an idea of what it would look like. I would have so much fun reading that. Please, somebody get it.

POSTED BY GEORGE HOTZ AT 8:23 AM

FRIDAY, AUGUST 10, 2007

Where we stand now...

We have three pretty much stalled approaches right now:
Cerberus--IO_SUPERVISOR still doesn't work. Find a datasheet or a PMB8876 tool. Latest tool code is here.
SAMPLE/PRELOAD--These are the raw dumps from the I/O pins. I don't have anyway to understand them. Find a datasheet.
Stack in Trace mode--This is where I am focusing now. This is hopefully the stack of the running chip, but it's a mess. We need some good reversers to look at this.

And we need new approaches. I know a lot about this hardware, and can find just about anything. Like I could find the H5 debug or the network port. But what good would it be. These things all connect to the logic chip, which we already have full control over. We need new ways into the S-Gold2.

I have a surefire unlock, but it'd be a *real* hack. We could remove the NOR chip, download a modified firmware to it, and put it back. Or we could just remove it and connect an FPGA in it's place. Then we could run whatever code we wanted. Including a hacked firmware.

POSTED BY GEORGE HOTZ AT 9:44 AM

---

2 COMMENTS:

Night said...

nice job!!! i want to help to u and the dev team, please collaborate to my blog.
http://iphonedonation.blogspot.com/

AUGUST 10, 2007 3:30 PM

Bruce said...

How about monitoring memory access on the NOR when the unlock code is checked, this could give you an idea of where the unlock code is stored. Also you could find where the counter for incorrect tries is stored.

SATURDAY, AUGUST 11, 2007

!!Call for ARM Reversers!!

I am setting aside JTAG for now until we come across more information. We have an idea for an attack on the baseband, but we need people who can reverse well. Basically we need people who are *very good* with ida. PM geohot on undernet if you think you can help.

POSTED BY GEORGE HOTZ AT 3:14 AM

SATURDAY, AUGUST 11, 2007

T-Mobile Sim Fully Working using JTAG

First, this is a bootleg hack, and isn't by any means an unlock. But it does work. The original idea of disabling the sim detect switch was brought to me by florin_m, and the idea is you boot with a valid sim then switch it. Thanks to JTAG I found out that the SIM is polled every second or so. So even if the detect switch is disabled, the phone still won't work with the new sim card. But here is a little trick, although impractical, to get a phone working with another sim.

Boot phone or AT+XSIMSTATE=1 with an AT&T SIM. It doesn't have to have service.
Halt the core with jtag(EXTEST all 1's)
Replace sim with any other SIM with valid service
Resume core with jtag(EXTEST back to old state)

Now it should work with any SIM. This functions similar to a SIM proxy without the SIM proxy hardware being required. But instead you need the JTAG hardware, which is arguably harder to get. Unfortunately a software halt won't work as the SIM is polled in an interrupt which still runs.

POSTED BY GEORGE HOTZ AT 5:44 PM

---

3 COMMENTS:

Philipp said...

so, do I understand fly, that you'd need to open up the phone for this to work?

AUGUST 11, 2007 7:23 PM

bajo said...

Yes. Look through the blog archive to see how to connect to the JTAG interface.

AUGUST 12, 2007 2:35 AM

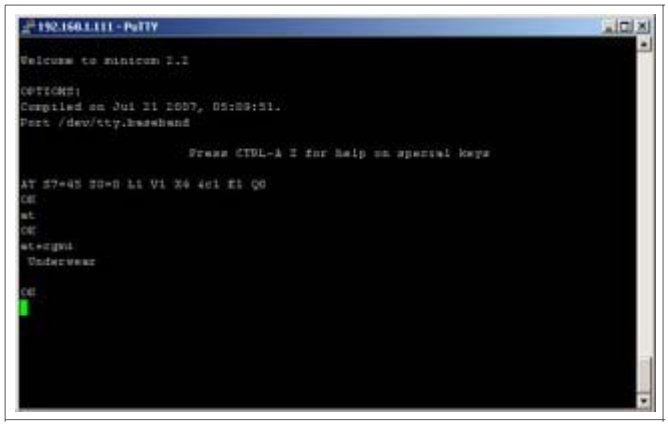
HaRRo said...

Sux0rs

AUGUST 12, 2007 7:57 AM

SUNDAY, AUGUST 12, 2007

Ha Ha



They really don't do a good job checking the signature of the EEP

POSTED BY GEORGE HOTZ AT 9:17 AM

---

7 COMMENTS:

Philipp said...

Aaaaaaahhhh.... why do I NEVER know what any of this means? LOL

I just want it to be unlocked already. How many more days? ;-)

AUGUST 12, 2007 10:21 AM

Juggler said...

To my knowledge, geohot just found a way to upload a eeprom file to the baseband. At+cgmi is supposed to give you the manufacturer identification information.

See:

http://iphone.fiveforty.net/wiki/index.php/Baseband

and

http://iphone.fiveforty.net/wiki/index.php/AT_Commands

AUGUST 12, 2007 11:33 AM

MONDAY, AUGUST 13, 2007

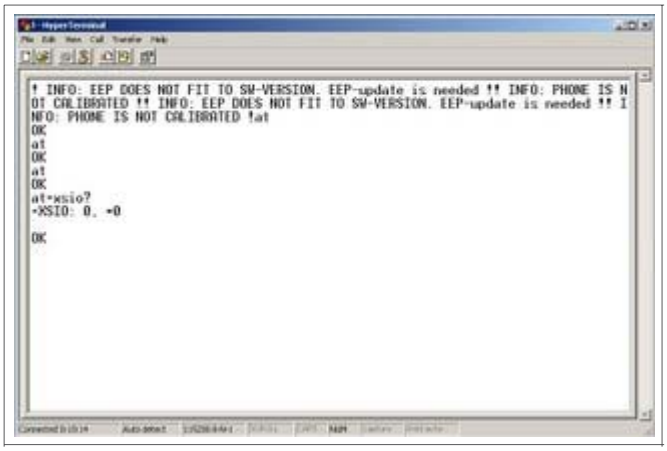
Some Chip Internals

iProof PMed me this morning with some new information, and it seems to be correct. First, he found a register list, which at least matches up for USART0. Also there is a bootrom at 0x00400000 which loads in case the flash isn't working. This is our new in. It should allow a full reflash without any sig checking. Although the protocol for the bootrom doesn't seem to match the Siemens phones.

POSTED BY GEORGE HOTZ AT 9:48 PM

MONDAY, AUGUST 13, 2007

AT Commands from the Computer



I connected up a level converter board to the UART found earlier. I cut tx coming from the logic board to stop the signals from conflicting. The lag came from minicom, so this interface is instant.

POSTED BY GEORGE HOTZ AT 11:17 PM

TUESDAY, AUGUST 14, 2007

NORtool

This is the start of a universal nor access tool using interactive mode of the bootloader. Have fun, I'll release the executable file at a later date when I feel it is mature enough to do so. It needs to be linked with IOkit. This was written by reversing the dev team's NORdumper.

POSTED BY GEORGE HOTZ AT 11:10 AM

---

2 COMMENTS:

helpgiver said...

Wish you would stop saying "interactive mode" like repetitive parrot. You still don't get it do you, look closer young Geo, look closer! Heh-heh, you never did get this to work did you? Now you might!

AUGUST 14, 2007 11:58 AM

Brazuca said...

well, this is a puzzling exchange.

AUGUST 14, 2007 1:52 PM

TUESDAY, AUGUST 14, 2007

Dump 0x00400000

This is the bootrom, and the key to full nor access.

POSTED BY GEORGE HOTZ AT 5:06 PM

---

4 COMMENTS:

HKara said...

Way to go. So is full sim unlock the next thing? Say yes please!

AUGUST 14, 2007 5:08 PM

Philipp said...

Yeah please... :-) Plain english for us followers hahaha. I'm trying to decide if I should invest in a TurboSim or if the unlock is just around the corner...

AUGUST 14, 2007 6:43 PM

Fernando said...

Way to go! It's awesome to be able to read your advances.

So, does this mean it will be possible to get a RAM dump, and then exploit a software weakness?

AUGUST 14, 2007 7:00 PM

Hakim Bennis said...

George,

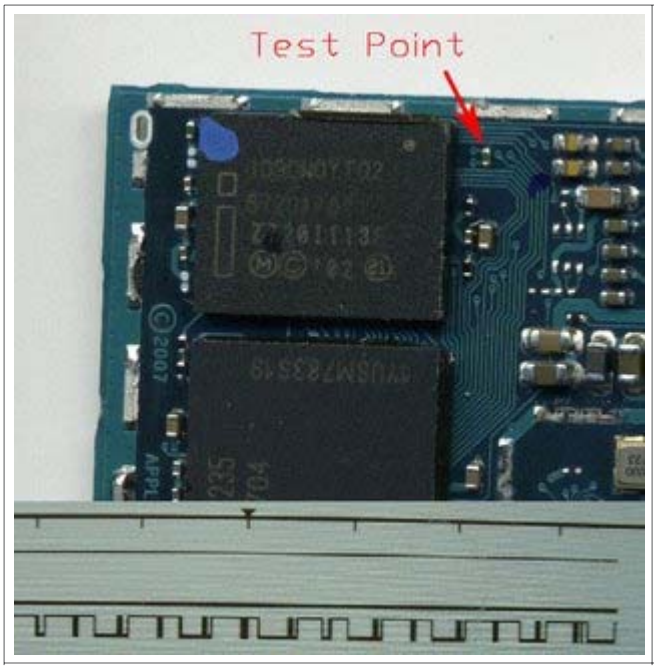
Please tell us when do you expect a FULL software unlock.
Everyone at my company is asking me everyday:
So did you unlock your phone, did you unlock your phone ??
....,

I'am sick of it!

AUGUST 15, 2007 8:08 AM

WEDNESDAY, AUGUST 15, 2007

Booting from the Bootrom



The key, at least in the Siemens phones, to getting the S-Gold2 to boot from the BootROM, is to disable the flash. The BootROM is believed to check for "CJKT" @ 0xA000003C then boot from the address @ 0xA0000038 So if it can't find that CJKT then it will boot into recovery mode. That "testpoint" is #R_OE so pulling it low will enable the ram outputs, effectively disabling the flash ones. But the Siemens protocol to access the bootrom doesn't seem to be working. The logic analyzer picture is what TX from S-Gold2 looks like, so something is definitely running. We need to dump it(0x00400000) and reverse it.

POSTED BY GEORGE HOTZ AT 4:13 AM

---

2 COMMENTS:

HaRRo said...

oooooooooo

AUGUST 15, 2007 12:16 PM

Philipp said...

Awwww.... where are the daily updates? Vacation? :-)

AUGUST 17, 2007 9:31 AM

SATURDAY, AUGUST 18, 2007

The Unlock Switch

POSTED BY GEORGE HOTZ AT 10:42 PM

---

5 COMMENTS:

David Christopher Bistolas said...

Care to explain?

AUGUST 18, 2007 11:56 PM

Yin said...

Hmmm...does this mean i have to get a vice, switch and some crocodile clips and hopefully i can unlock my iphone :) BTW cool setup hahaha.

AUGUST 19, 2007 12:18 AM

Fernando said...

??

AUGUST 19, 2007 2:03 AM

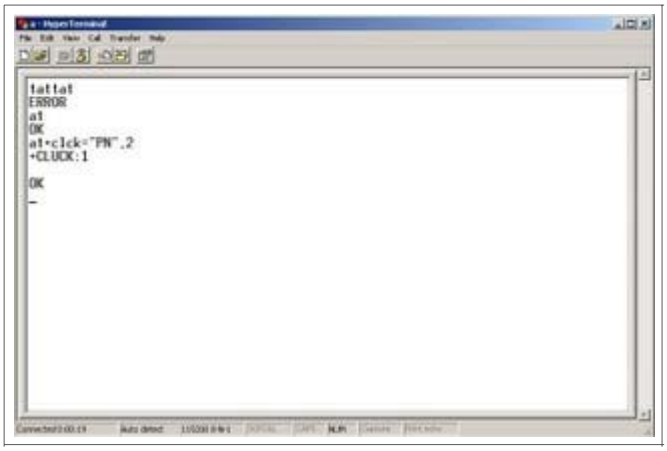
Philipp said...

Explanation... pleeeeease :-)

AUGUST 19, 2007 4:34 AM

SUNDAY, AUGUST 19, 2007

Your iPhone can CLCK, but can it CLUCK?



Just to clarify, CLUCK is the noise a chicken makes and nothing more.

POSTED BY GEORGE HOTZ AT 11:06 AM

---

3 COMMENTS:

Trax said...

Dude, your killing us

AUGUST 19, 2007 2:39 PM

ag886 said...

http://www.thecluck.org/

AUGUST 19, 2007 2:46 PM

xPhone said...

I think the good George finally has gone over the edge. All those nights without sleep trying to hack the iPhone was to much. Now ha has gone all cuckoo.

The duke had a mind that ticked like a clock and, like a clock, it
regularly went cuckoo.
-- Terry Pratchett, Wyrd Sisters

AUGUST 20, 2007 4:55 AM

MONDAY, AUGUST 20, 2007

Allowed MCCMNC's

310-150
310-170
310-410
001-010
311-180
310-980
Thanks to gray who has been reversing the main fw for finding this.

POSTED BY GEORGE HOTZ AT 12:00 PM

---

6 COMMENTS:

Trax said...

310 United States 150 Cingular Wireless
310 United States 170 Cingular Wireless
310 United States 410 Cingular Wireless
311 United States - 180 Cingular Wireless
310 United States 980 AT&T Wireless Services Inc

Now I couldn't find what 001-010 are for.
Do these MCCMNC mean you have to be on such a country/operator combination to be able to enter an unlock code?

AUGUST 20, 2007 6:11 PM

John said...

001-010 is a "Test SIM card". There is no real network associated with it.

AUGUST 20, 2007 7:46 PM

John said...

This post has been removed by the author.
AUGUST 20, 2007 7:50 PM

TUESDAY, AUGUST 21, 2007

FULL HARDWARE UNLOCK OF IPHONE DONE

Video

Yes thats right, we have an unlocked iPhone. The hardware is only used to unlock the iPhone, and can be removed after it's unlocked. Thanks to gray, iProof, geohot, dinopio, lazyc0der, and an anonymous contributor for making this possible. Thanks also to everyone who donated and stuck with us in #iphone.unlock. Our group has agreed to release the method in one week. The current method involves taking apart your phone and doing some complicated soldering, with a high probablity of a bricked phone. Although after the phone is unlocked all the hardware can be removed. We hope to find a software unlock very soon. So in one week exactly from this blog post(thats less than the time it takes to ship a turbosim) we will release simple step by step instructions for unlocking, probably not even involving hardware. Sorry about the wait, but I assure you it will be worth it.

POSTED BY GEORGE HOTZ AT 11:51 AM

---

68 COMMENTS:

Dave said...

Congrats dude.

AUGUST 21, 2007 12:09 PM

Mickie said...

Well done Geo

AUGUST 21, 2007 12:18 PM

Brazuca said...

Can't I just glue on a big red "unlock switch" to my iPhone?

Why not?

AUGUST 21, 2007 12:24 PM

THURSDAY, AUGUST 23, 2007

ITS RELEASE TIME

Welcome to the final countdown. I am leaving for college Saturday, and have been busy lately with getting everything ready. And once I am there, I really won't have much time to work on the iPhone. But I don't want to leave being the only person with an unlocked iPhone :) So we have decided to release the hardware unlock. The hardware required is decently simple, and most people who have modded a game system have the soldering ability required to do it. This has been a great adventure, the "summer of the iPhone", and I finally achieved my goal of getting my phone working on T-Mobile. So its about time everyone else can do this too. Here is the release plan. Last night, I went to the Apple store, and purchased a brand new 4GB iPhone. At 8AM EST sharp, I will begin unlocking a NIB iPhone step by step on the blog along with everyone who wants to come along. I'll be answering any questions on #iphone.unlock @ undernet. I'll be doing the hardware part first, so you can wait to see if you think the hardware is too complicated before diving in and taking apart the phone. But it really is only a wire that needs to be soldered. So see you all at 8 AM EST.

POSTED BY GEORGE HOTZ AT 5:51 AM

---

3 COMMENTS:

TOSSAPORN said...

This post has been removed by the author.
AUGUST 23, 2007 5:58 AM

TermServ said...

I'm not really on IRC, so are you going to post a tutorial or summary? (Pretty please?) ;)

AUGUST 23, 2007 6:32 AM

AC said...

Does that mean there will be a Software method ??

AUGUST 23, 2007 7:28 AM

THURSDAY, AUGUST 23, 2007

What you need

--First, an iPhone. Of the sshed and jailbroken variety. Also, kill commcenter by moving the LaunchDaemon plist out of the directory.
--Some trusty case opener tools(read: guitar picks) Read one of the many tutorials available online for taking apart your phone.
--A soldering iron. This should've cost you more than $10.
--Fine pitch wire. I used magnet wire salvaged from a little motor.
--An unlock switch. The bigger and more badass, the better. Or if you are cheap, wire cutters :-)
--A red bull. This requires concentration, something I don't have without Red Bull.

POSTED BY GEORGE HOTZ AT 6:07 AM

---

2 COMMENTS:

MJR said...

George - don't go back to school yet - we fat finger solderers need a software unlock :-)

Thanks for all your work
I'd love to hire your entire team

AUGUST 23, 2007 6:25 AM

THURSDAY, AUGUST 23, 2007

Some Comments on the Method

This method is very similar to the method used to unlock the Siemens phones with the S-Gold2 chipset. The S-Gold2 has a bootrom which allows you to download a bit of unsigned code. This code is run if certain flash addresses are blank. Using a little hardware trick, which I'll explain later, we make them appear blank. Then once we have unsigned code running on the baseband, we can download a modified firmware, with the unlock patched in, to the nor flash. The signature checks only cover this region while it is being downloaded the first time. Once the code is on the NOR we can do whatever we want. So patch out the PN lock; Voila, unlocked iPhone.

POSTED BY GEORGE HOTZ AT 6:23 AM

---

9 COMMENTS:

Alexander said...

nice
thank you geo :)

AUGUST 23, 2007 6:34 AM

Cato said...

Awsome! Keep the descriptions coming!

AUGUST 23, 2007 6:40 AM

MJR said...

Would you have to re-unlock with each firmware upgrade ?

AUGUST 23, 2007 6:51 AM

david said...

Oh...I look forward to the software version. It's tempting to try this however.

AUGUST 23, 2007 7:25 AM

THURSDAY, AUGUST 23, 2007

Step 1

First, I would like to say thanks again to gray, iProof, dinopio, lazyc0der, anonymous, the dev team, nightwatch, and everyone who donated. Without them, there would be no unlock today, and I surely wouldn't be up at 8AM.
Second, you may brick your iPhone using this tutorial. YOU ARE WARNED.
Okay on to the actual step. Remove the black part, the three screws, and the aluminum case. Disconnect the wire connecting the phone to the case. Do not remove anything else. Comment on these posts if you are with me so far. Once we get a good number of comments I'll move on.

POSTED BY GEORGE HOTZ AT 7:50 AM

---

17 COMMENTS:

Mike said...

COMMENT! STEP 2 PLSSSS

AUGUST 23, 2007 7:57 AM

Vicious said...

easy enough...

AUGUST 23, 2007 7:57 AM

THURSDAY, AUGUST 23, 2007

Step 2

Also remove the metal cover over the comm board. This is all the disassembly you have to do. If you feel like being safe, desolder the battery red lead. I didn't :)

POSTED BY GEORGE HOTZ AT 8:03 AM

---

12 COMMENTS:

drh said...

done.

AUGUST 23, 2007 8:05 AM

Vicious said...

wow drh your fast let me catch up

AUGUST 23, 2007 8:05 AM

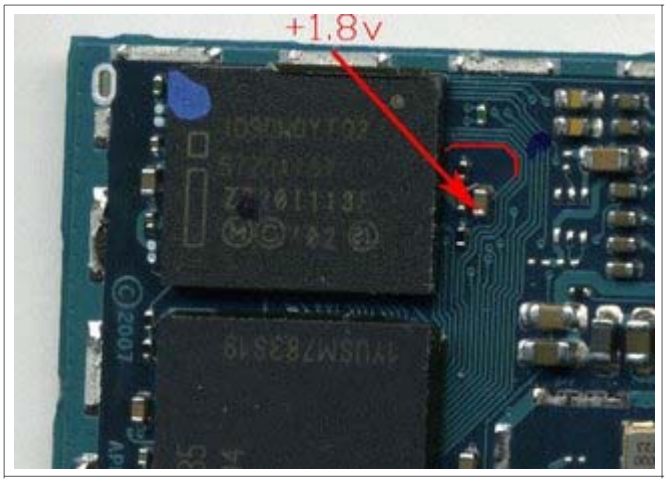
Steve said...

go go go please

AUGUST 23, 2007 8:06 AM

THURSDAY, AUGUST 23, 2007

Step 3



The red line is covering the A17 trace. In order to trick the chip into thinking the flash is erased in the correct section, you will need to pull this high. Scrape away at the trace with something like a multimeter probe. Then solder a very thin wire to it. Be very careful. Only scrape away at that solder mask above that one trace. YOU DO NOT WANT TO BREAK THE TRACE. This is the hardest step in the whole process; the rest is cake. Also solder a wire to the 1.8v line. Connect to wire coming from the trace and the wire coming from the 1.8v to your unlock switch. Be careful, you only get one chance to do this right. Thanks again to Nick Chernyy for the picture.

POSTED BY GEORGE HOTZ AT 8:14 AM

---

13 COMMENTS:

david said...

"pull this high"?

AUGUST 23, 2007 8:22 AM

drh said...

did i miss a bit ? where did we get 1.8v switching involved?

AUGUST 23, 2007 8:22 AM

Mike said...

this is where the redbull comes in, gentlemen.

AUGUST 23, 2007 8:27 AM

THURSDAY, AUGUST 23, 2007

My Finished Step 3

Hopefully yours will look like this.

POSTED BY GEORGE HOTZ AT 8:20 AM

---

5 COMMENTS:

david said...

Looks like you run the wires under the frame of the com board, is that correct? (more photos would be helpful!) Thanks.

AUGUST 23, 2007 8:26 AM

boss_khan24 said...

a video would be very help full.

AUGUST 23, 2007 8:27 AM

david said...

Are you snapping these with a 2MP iPhone? :-) Needs. more. macro.

AUGUST 23, 2007 8:29 AM

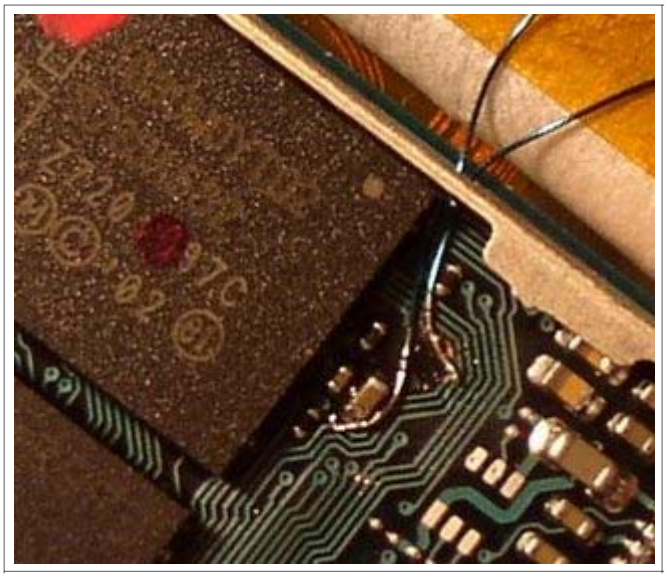
DarrelRodman said...

Ok, I'm here... what do I do next?

AUGUST 23, 2007 8:33 AM

THURSDAY, AUGUST 23, 2007

Zoomed In Step 3



You can do it. I believe in you.

POSTED BY GEORGE HOTZ AT 8:26 AM

---

24 COMMENTS:

boss_khan24 said...

hey dude where do you live? you know if you start doing this for ppl like even just 10 a week! thats like 500 to 1000 for you in your pocket right there!

or make a software unlock lol and sell it for like 20.

YOu will make like 10 grand ez

AUGUST 23, 2007 8:30 AM

marc.haberland said...

This post has been removed by the author.
AUGUST 23, 2007 8:30 AM

boss_khan24 said...

This post has been removed by the author.
AUGUST 23, 2007 8:31 AM

THURSDAY, AUGUST 23, 2007

Step 4

Ok, time to test what you just soldered. First use the continuity check on a multimeter to make sure the wires aren't shorting to ground or to each other. Make sure your switch is in the off position. Power up your iPhone. Hopefully it didn't smoke :)
Now go into minicom to tty.baseband and send a few commands, AT a few times will do. It should respond OK. Now flip your switch, the baseband should stop responding. Even when you flip it back, the baseband still shouldn't respond. Be sure your switch is off, then open another ssh and run "bbupdater -v" You can get bbupdater off the ramdisk. This should reset the baseband, and minicom should start working again. If it did this, your soldering is most likely good, and you are ready to actually start unlocking your phone!!!

POSTED BY GEORGE HOTZ AT 9:44 AM

---

22 COMMENTS:

Diet said...

Hi geohot, great work!
Just a little question: how do I use minicom? Via ssh directly on the iPhone? Didn't find a detailed description about this step!
Thanks a lot, Diet

AUGUST 23, 2007 10:00 AM

david said...

http://www.macosxhints.com/article.php?story=2004102611330

AUGUST 23, 2007 10:06 AM

Diet said...

Thanks! Just found out that minicom is already on the iPhone. The only problem is that it's trying to connect /dev/modem when started (minicom: cannot open /dev/modem: No such file or directory). Running minicom with the parameter /dev/tty.baseband doesn't work. Any hints?

AUGUST 23, 2007 10:15 AM

THURSDAY, AUGUST 23, 2007

Step 5

If it passed the checks in step 4, congratulate yourself. You are a pro solderer. Go eat lunch. If not, don't worry yet. I must've thought I bricked my phone 100 times. First of all, to power up your phone you don't need to reconnect the case with the power button. Just connect it with USB, it'll power itself up. Secondly, don't waste time compiling minicom. Download the binary here, and termcap here.

POSTED BY GEORGE HOTZ AT 11:31 AM

---

9 COMMENTS:

gqdev said...

its 8:37AM here in LA.. I can't eat lunch ... what's the progressssssss

AUGUST 23, 2007 11:38 AM

mokum von Amsterdam said...

It's 17:39 here on the old continent and I could not care less about food in any which way :P
Keep up the good work [and people make a mirror of this for it will sooner or later be removed...

AUGUST 23, 2007 11:41 AM

mycintosh said...

Oh Jeees' ... a little bit un-nerding would be great.
I don't get it at all ...

Somebody willing to translate this manual for mere mortals?

AUGUST 23, 2007 11:44 AM

Pitou said...

for those who are worried that it'll be deleted, i copied down everything...

AUGUST 23, 2007 11:45 AM

THURSDAY, AUGUST 23, 2007

Step 6

Now, with the switch off, your baseband should be working perfectly. Here you should take a NOR dump of your phone. The dev team's NORDumper is a great way to do this. This is good to have in case something goes wrong. You can extract the firmware from this as well, which we'll get to later.

POSTED BY GEORGE HOTZ AT 12:09 PM

---

5 COMMENTS:

gqdev said...

how many more steps left..

AUGUST 23, 2007 12:15 PM

George Hotz said...

idk, maybe 40, but some might be NOP

AUGUST 23, 2007 12:18 PM

info said...

In Italy working on 3 iphone in same time...
only 6 red bull left :-)
great job.. tk a lot.

AUGUST 23, 2007 12:23 PM

Mike said...

you need more red bull than that ;)

AUGUST 23, 2007 12:48 PM

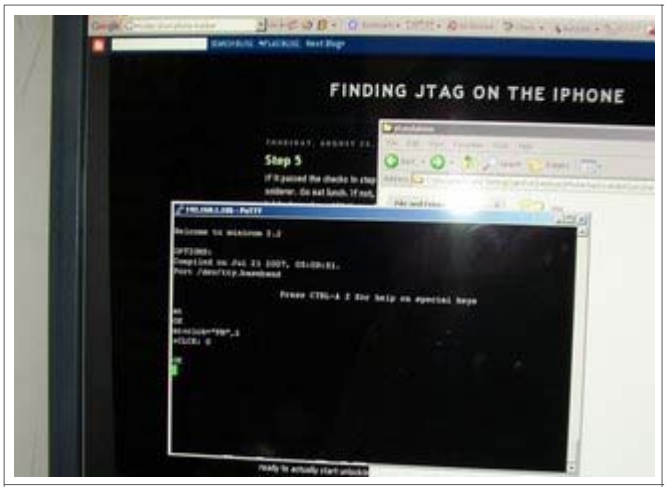
Antonio said...

@info: do you want to add another phone to your chain? I'm from italy too :-)

AUGUST 23, 2007 12:48 PM

THURSDAY, AUGUST 23, 2007

A Little Motivation



This is the world's second (outside super secret apple vault) unlocked iPhone.

POSTED BY GEORGE HOTZ AT 12:37 PM

---

5 COMMENTS:

Bart said...

Setting up your interview with the Today show? ;)
Let us know when :)

AUGUST 23, 2007 12:45 PM

Alexandre said...

Congratulations, and thank you for this job.

Big thanks to the whole team

svcadg11

AUGUST 23, 2007 12:47 PM

Tommaso said...

I'm not sure if I understood all the tech stuff, but I believe that this hack can be voided by Apple with an iPhone update. Is it right?
Thanks!

AUGUST 23, 2007 12:48 PM

THURSDAY, AUGUST 23, 2007

Think of how pretty it'll be...

POSTED BY GEORGE HOTZ AT 1:13 PM

---

6 COMMENTS:

Mike said...

does this mean there will be no software unlock coming from you dude?

AUGUST 23, 2007 1:16 PM

Mike said...

you will never know ;)

(dude you're using my name! -p9939068)

AUGUST 23, 2007 1:20 PM

Mike said...

lol sorry about that, it just so happens to be my name too, i take it now that geohot has released his step by step unlocking, and its a hardware method he wont be releasing a software unlock on tuesday?

AUGUST 23, 2007 1:23 PM

Diet said...

@geohot: did you manage to open your iPhones without scratches or other traces? That's what I'm afraid of most ...

AUGUST 23, 2007 1:24 PM

THURSDAY, AUGUST 23, 2007

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

---

18 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

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

---

2 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

THURSDAY, AUGUST 23, 2007

Step 9

The final tool is iUnlocker. This tool uploads a small program, "testcode.bb", to the baseband using the bootrom exploit. This program needs to be in a dir with "nor", the file you obtained in the last step. You need to have the switch on when running this program. This will download and run the code in "testcode.bb" Then the program will stop and ask to to turn off the switch. Do so. You type any character then hit enter. The nor download starts right away. When the counter reaches 0x2E4000, it is done. Run "bbupdater -v". Hopefully it will return the xgendata. If is does, the nor upload was successful.

POSTED BY GEORGE HOTZ AT 3:00 PM

---

2 COMMENTS:

rteng said...

Is this the only spot where the switch needs to be on?

AUGUST 24, 2007 2:47 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

THURSDAY, AUGUST 23, 2007

Step 10: The Last One

minicom into /dev/tty.baseband. If you already used up your attempt counter, the phone should already be unlocked. If not just run 'AT+CLCK="PN",0,"00000000". That will unlock the phone for sure. Run 'AT+CLCK="PN",2'. It should finally return 0!!!
Your phone is now unlocked. Exit minicom and copy the CommCenter plist back to its place. Reboot. iASign. And enjoy your unlocked iPhone.

POSTED BY GEORGE HOTZ AT 3:10 PM

---

32 COMMENTS:

Terje said...

Awesome! Good work geohot!

Now give us the softmod soon ;-)

AUGUST 23, 2007 3:15 PM

david said...

You lost me about 5 steps ago, but I am thrilled to think that someone might be able to generate a softhack based on what they are learning tonight. Thanks again, geohot, and good luck starting school.

AUGUST 23, 2007 3:18 PM

ag886 said...

Geo,
if they modem firmware changes in the patch, like it did 1.0->1.0.1 will this require to re-unlock the phone ?
Thanks
AG

AUGUST 23, 2007 3:26 PM

mokum von Amsterdam said...

Pretty nifty work.
My compliments to the crew.

AUGUST 23, 2007 3:32 PM

THURSDAY, AUGUST 23, 2007

Postmortem

So if you follow these steps, you should have an unlocked iPhone. I'm sorry about how hard they are to follow, but someone will get them to work, and simplify them, and simplify them more. Hopefully a software unlock will be found in the near future.

I'm sorry to say I won't be in the iPhone scene anymore. I leave for college in two days, and I have so much to do. We still have a good amount, about a grand, of donation money left. We definitely need to buy jpetrie a new iPhone. He donated the original phone that made all this possible. I'll even unlock the new phone for him. With the money left over, if anyone wants it back, drop me a line. I wish I had time right now to unlock iPhones for people, but even with this method it'll take me two hours per phone, and I'm leaving so soon. I will continue to post to this blog, and I will continue to work with the iPhone, but not on a software unlock. I am pretty much useless there. I plan on setting up a ssh box into my test iPhone for gray to play around with. In these posts/files is basically everything I know. I have a few cool ideas for things I want to do with the phone, like a cell phone tower based gps. I will detail everything on this blog.

Using this exploit is should be very easy to permanently mod your phone to run unsigned code. Just write 0xFFFFFFF to the locations the bootrom checks. I don't believe they are used. Also, if anyone finds a way to erase the bootloader from software, this becomes a software unlock.

I really wish I had more time to detail all of this, and one day I will. You will always be able to reach me at geohot at gmail. This has been a great community and has been a great trip. I hope I was a positive influence on the community. Thanks so much everyone, I have learned so much. Coming into this project I didn't know that cell phones used at commands, or that there was a distinction between kernel/user space. I had once in my life looked at ida before this, and found it too confusing. I still can't reverse well, but this is definitely something I want to learn. Thanks again everyone.

POSTED BY GEORGE HOTZ AT 3:15 PM

THURSDAY, AUGUST 23, 2007

The Energy it took...

POSTED BY GEORGE HOTZ AT 4:04 PM

---

40 COMMENTS:

Jeroen said...

omg!

AUGUST 23, 2007 4:10 PM

gqdev said...

dudeeeee.. u must be shaking cuz u havent slept ... and those many redbulls ... i dont knowwww..

AUGUST 23, 2007 4:11 PM

Jay said...

congrats and THANK YOU for all the hard work. good luck in school and with all you do in the future.

AUGUST 23, 2007 4:28 PM

jszeto said...

congrat! I'm going to do it too.. but do I needed to use Mac, or windows is ok? Does the NORDumper can use on windows ?

All the Best!!

AUGUST 23, 2007 6:20 PM

THURSDAY, AUGUST 23, 2007

The Phone is for sale

eBay Auction

This is the phone that was unlocked live here this morning. It includes the phone, the worlds first serial dock, and the official unlock switch from the blog.

As a note, if you are only bidding on this to get an unlocked iPhone, don't. There are much cheaper and easier ways to get one. This is a piece of cell phone history. I have no intention of ever starting an unlocking service.

I'm sure these most recent bids are fake. I have a confirmed offer of $25,000 and an unconfirmed offer of $100,000. If you are willing to buy it for more, please post your phone number+email address+what you'd pay in a blog comment and I will contact you

POSTED BY GEORGE HOTZ AT 8:32 PM

---

308 COMMENTS:

7777 said...

Hello
I would like to buy your fone.How much do you want?Please give me a price for it to bao789789@yahoo.com,and i need to talk with you by yahoo massenger bao7897892001@yahoo.com or at gtalk baonguyen
Let me know soon
thanks

AUGUST 23, 2007 8:40 PM

luis said...

650 usd what do you say geo by the way thanks

AUGUST 23, 2007 8:43 PM

Mike said...

a pity it's not an 8gb :(

AUGUST 23, 2007 8:49 PM