12-4-2007

Taxonomy of iPhone Activation and SIM Unlocking Methods

Marwan Al-Zarouni
Edith Cowan University

Haitham Al-Hajri
Edith Cowan University

DOI: 10.4225/75/57b53a26b8757
5th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, December 4th 2007.

Taxonomy of iPhone Activation and SIM Unlocking Methods

Marwan Al-Zarouni
Haitham Al-Hajri
School of Computer and Information Science
Edith Cowan University
iPhone@marwan.com
Haitham@MySecured.com

Abstract

This paper will discuss the different methods of SIM unlocking and activation for the Apple iPhone. Early iPhone activation and SIM card fabrication methods as well as the latest software only methods will be discussed. The paper will examine the benefits and drawbacks of each method. It will provide a step-by-step guide to creating a specially crafted SIM card for an iPhone by using Super SIM and Turbo SIM methods. The paper will also include a section on recovering (unbricking) the iPhone and other advanced hacks.

Keywords

iPhone Activation, iPhone Hacks, iPhone SIM Unlock, iPhone Unlocking, Super SIM, Turbo SIM.

DISCLAIMERS

The Authors of this paper do not claim any responsibility, legal or otherwise for the use or misuse of instructions or any information provided within this paper. All information provided is for educational purposes ONLY. Some of the hacks may be illegal in some countries and may violate Apple's software copyrights and other intellectual property laws. Do not attempt this with your own iPhone.

BACKGROUND INFORMATION

The Apple iPhone is arguably one of the most hyped and anticipated gadgets of all time(TMHGIH 2007). The reason for the hype is that the iPhone has an enhanced graphical user interface implementing multi-touch technology that recognizes multiple simultaneous touch points on a large LCD screen. This in addition to many other hardware and software features including interactive Google maps, stock quotes, weather, built-in camera and a Safari web browser. The iPhone also boasts a powerful Mac OSX based Operating System (OS) which is superior to many mobile phone operating systems that are currently on the market. The iPhone is considered by many as a revolutionary device with more than 300 patents filed by Apple (Apple 2007b).

Before its release, Apple announced that the phone will be sold un-activated and that it will have to be activated through iTunes software by signing a two year contract with the Unites States based telecommunications company AT&T. This type of activation will hereafter be referred to as the "iTunes-AT&T Activation". It involves iTunes getting a unique 40 digit DeviceID from the iPhone, the phone hardware's unique International Mobile Equipment Identity (IMEI) number, and the Integrated Circuit Card ID (ICCID) serial number from the SIM card shipped with the iPhone. This information then forms a unique token which is sent to the apple server (alfred.apple.com) via SSL. Apple then uses their private key to sign the token and transmits it back to iTunes. iTunes on the user's computer then calls AMDeviceActivate with this signed token. Finally, the device gets the token and checks whether or not the signature matches the token. If it does, the device is activated (DevWiki 2007).

The reason behind requiring the iPhone to be activated before use is because Apple, the manufacturer of the iPhone, signed a five year exclusivity agreement with AT&T for phone service rights on the iPhone (Cauley 2007). Thus, an iPhone buyer must sign a contract with AT&T before he or she can start to use any of the phone's features. The picture below shows a brand new iPhone screen once it is turned on and before activating it with iTunes-AT&T Activation (Figure 1).

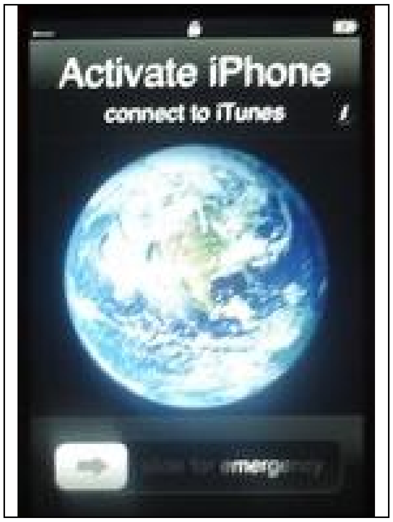


Figure 9: An out of the box iPhone screen showing "Activate iPhone connect to iTunes".

ITUNES-AT&T ACTIVATION AND SIM LOCKING

Apple and AT&T went to great lengths to insure that the iPhone can only be activated with the iTunes-AT&T Activation method. Activation then enables the user to access all phone functionalities including the main features such as phone, SMS, Visual Voicemail, and YouTube.

iPhone's phone-related functionalities are however locked to the AT&T Subscriber Identity Module (SIM) card which is pre-installed within every iPhone sold in the United States. The picture below shows where the SIM card is located. The tray containing the AT&T SIM card can be ejected by inserting an unfolded paper clip into a tiny hole on top of the iPhone (Figure 2).

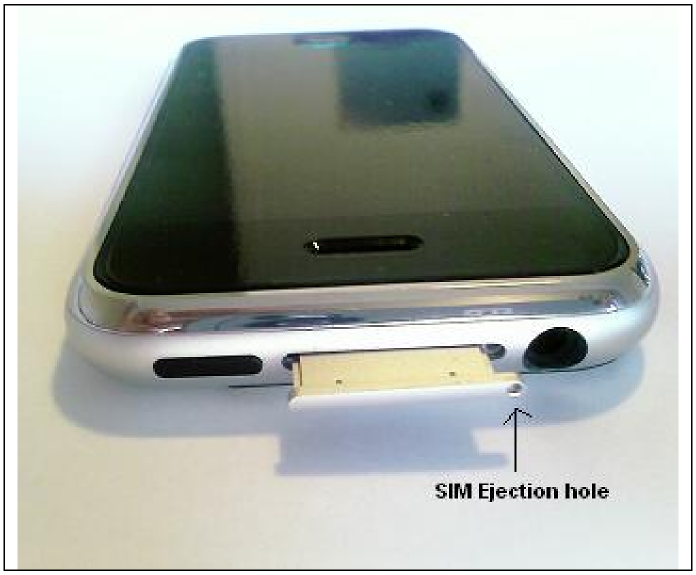


Figure 10: The iPhone SIM tray and slot that contains an AT&T SIM card.

Therefore the iPhone cannot be used with SIM cards from other phone service providers even after the phone is activated with AT&T. The AT&T-only SIM card locking of the iPhone will hereafter be referred to as iPhone's "SIM Locking". Using a SIM card other than phone's AT&T SIM card will result in an “Invalid SIM Error”. This is because the Phone checks to see if the International Mobile Subscriber Identity (IMSI) of the SIM card inserted in it matches AT&T. If it doesn’t, the iPhone shows the error and then blacks out the iPhone screen. The only way to activate the iPhone again is to replace the AT&T SIM card in the phone and restart it

THE PURPOSE OF THE PAPER

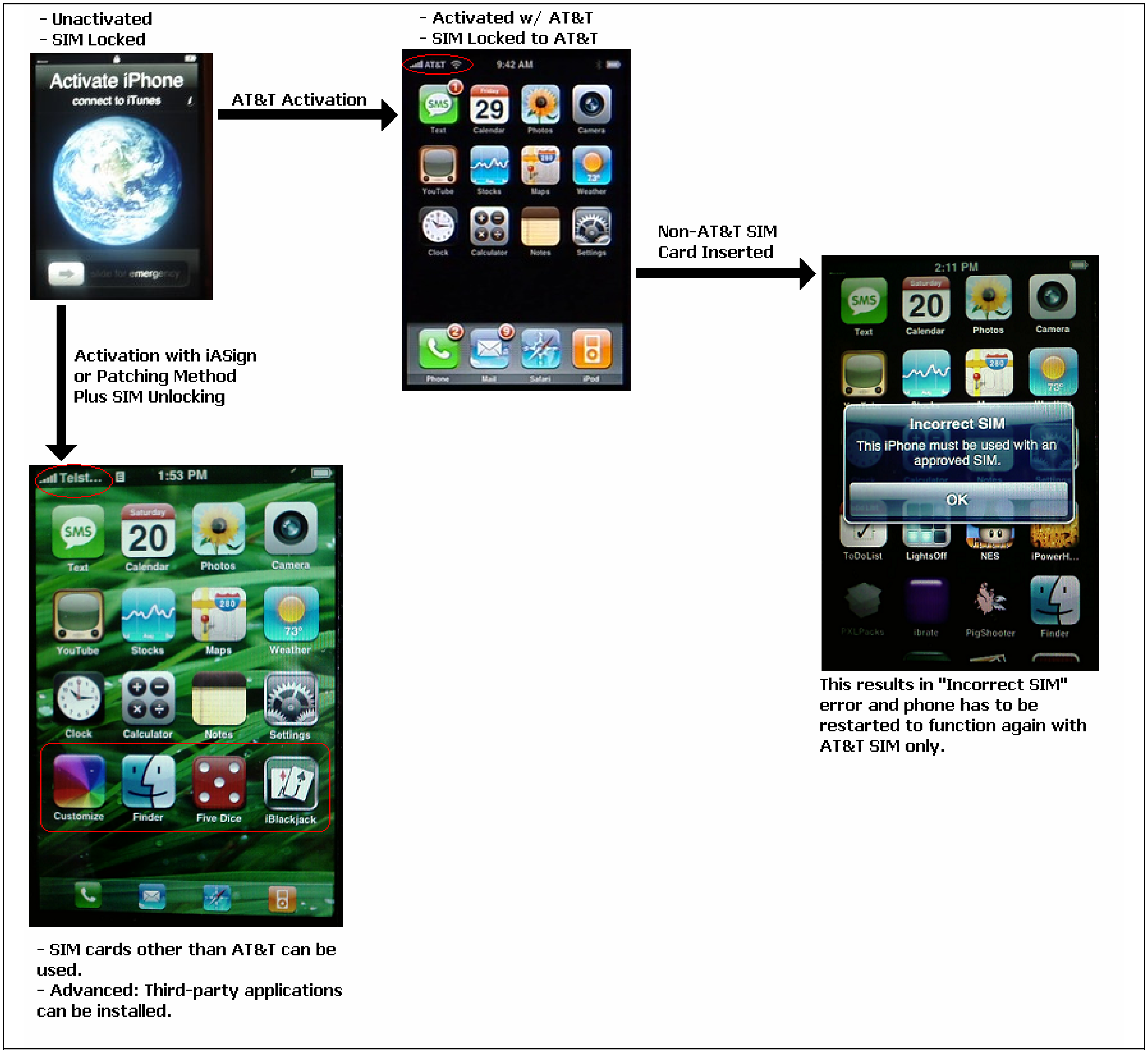
The hacking community and iPhone fans around the world wanted to use the iPhone functions without being bound to a two year contract with AT&T. Furthermore, people outside the United States who did not have the option of signing-up with AT&T wanted to enable Phone, SMS messaging, and GPRS (EDGE) and other service-provider-based functionalities of the iPhone with their own provider's SIM cards. This led people to come up with hacks to bypass the restrictions put on the iPhone. The purpose of this paper is to highlight the methods of hacking the iPhone and show the advantages and disadvantages of each of them.

THE DIFFERENCE BETWEEN ACTIVATION AND UNLOCKING METHODS

In order for someone to use the iPhone without using the AT&T SIM card, the phone needs to be activated and/or SIM unlocked. Here are the definitions of the terms:

- **Activation**: This means that the phone functionalities will be enabled. It may also mean that the user is able to install third-party applications and ring tones on the iPhone. Activation does NOT however mean that SIM card related functionalities will be enabled.
- **SIM unlocking**: This means that SIM cards other than the AT&T SIM card associated with the phone can be used to make calls, SMS and use GPRS functions of the iPhone.

Figure 3 shows iPhone screen shots during different stages of activation and SIM unlocking. The first screen shot on the left is for a brand new iPhone before any type of activation. The phone is locked and can only be used to make emergency calls. No other functions on it can be used. The next screen shot is of an AT&T activated iPhone that is fully functional when an AT&T card is inserted in it. The AT&T carrier logo can be seen on the top left corner of the screen shot. The screen shot to the far right shows the AT&T activated iPhone but with another SIM card inserted in it. This results in the iPhone refusing to work anymore and presenting an "Incorrect SIM" error. The screen shot on the bottom left shows a hacked iPhone that is both activated and SIM unlocked and working with a Telstra SIM card as shown in the top left of the screen shot. The phone also has third party software installed on it as shown in the bottom raw of icons on its screen.



Incorrect SIM

This iPhone must be used with an approved SIM.

OK

This results in "Incorrect SIM" error and phone has to be restarted to function again with AT&T SIM only.

- SIM cards other than AT&T can be used.
- Advanced: Third-party applications can be installed.

Figure 11: Screen Shots of brand new iPhone AT&T activated iPhone with and without AT&T SIM card, and Activated plus SIM unlocked iPhone.

iPhone Hacks Timeline

The following is a timeline of some of the most popular iPhone hacks and activation methods that surfaced science the iPhone was released on the 29th of June:

Hack Name	Hack Level	Date Released (approximate)
DVD Jon Activation	Activation Only	3 July (Johansen 2007)
iASign Activation	Activation + Software Limited SIM Unlock	18 July (Sadun 2007)
Super SIM	Hardware Limited SIM Unlock	5 August (Sassha 2007)
Turbo SIM	Hardware Total SIM Unlock	14 August (Al-Zarouni 2007)
AnySIM	Software Total SIM Unlock	15 September (Johnston 2007)

Table 1: iPhone Hacks Timeline.

DVD Jon Activation

This was the earliest hack for the iPhone coming out as soon as a few days after the iPhone was released. It allowed for non SIM card related functionality only. The hack is based on fooling the iTunes software into thinking that a localhost based server is actually Apple's activation server and activating the iPhone in that way. The hack involves Hex editing the iTunes software and is limited to a certain version of iTunes software namely 7.3.0.54 (Johansen 2007).

iASign Certificate-Based Activation

The iASign activation method was created to enable people to use pre-paid AT&T or Cingular SIM cards with the iPhone so that the user will not be bound to a two year contract. This is why this method is sometimes referred to as the "Prepaid AT&T and Cingular Activation".

The method requires the iPhone to be "jailbreaked". Jailbreak means that the iPhone is put into a mode where files can be written to it. This is because the iPhone by default is shipped in read-only mode. A Jailbreak program is available for both Windows OS and Mac OS platforms. This method also involves swapping the original certificate file on the iPhone: "iPhoneActivation.pem" with a pre-fabricated one. The method can be done offline on a Mac machine or online for windows users. The site to visit is: https://ookoo.org/iphone/iasign.php which has a form in which the user is required to enter the following values: Device ID, IMEI, ICCID in order to generate an executable file that can be used to activate the iPhone (HTIP 2007). The ICCID in this case should be the ICCID for the Prepaid AT&T or Cingular card that the user will use with the iPhone. The advantage for this type of activation is that it is update proof up to firmware 1.0.2. The disadvantage however is that the phone can only be used with the SIM card with the ICCID used to generate the certificate. Moreover, the ICCID has to be of a SIM card issued by AT&T or Cingular.

This method can also be combined with the Super SIM unlocking method to achieve total unlock. This is done by entering the ICCID number from the original AT&T SIM associated with the phone and programmed into the Super SIM card into the iASign online form instead of the ICCID number from the prepaid AT&T or Cingular SIM card. Total unlock in this case means access to all phone features except for Visual Voicemail. Visual Voicemail is an AT&T network-dependent iPhone feature that allows iPhone users to go directly to any of their voicemail messages without listening to the prior messages (Apple 2007a).

Lockdownd Patching Activation

The idea is to bypass activation altogether. It works by patching the "lockdownd" file located on the iPhone in "/usr/libexec/lockdownd". It still requires the iPhone to be jailbreaked in order to get access to that file to read it, patch it on a PC and then replace it in the same directory afterwards. The patching program used in this case is "V_KLay patcher" which is a Russian program used to patch the firmware of Siemens mobile phones (ValeraVi 2007). The status of the phone then changes from "unactivated" to "FactoryActivated" so the phone does not check the certificate files.

The patching changes two values in the lockdown file to the following:

- ActivationState to FactoryActivated
- brick_mode flag to brickmode_off

The "lockdownd" file does not stay exactly the same with every update of the iPhone firmware. Therefore, this patching method is very dependent on the firmware version. This means that a patch for firmware version 1.0 will not be applicable for firmware version 1.0.1 or later. This method is not update proof either which means updating the patched phone from 1.0 to 1.0.1 will result in re-locking the iPhone.

On the other hand, and unlike iASign method, this method works with multiple SIM cards. It also does not need the original AT&T SIM card that came with the iPhone to achieve activation so it is ideal for:

- iPhone users who change SIM cards frequently
- Concurrent use of two SIM cards in the iPhone by using a special adapter that allows one SIM to be on standby and another one to be active
- iPhone users that lost the original SIM card associated with the iPhone
- People who do not want to give out their phone specific information to a web based form

The following table compares the features of each activation methods and their ability to withstand and support a firmware update or restore.

Activation Method	**Phone**	**SIM Support**	**Firmware Update Proof**	**Firmware Restore Proof**
Legitimate Activation	Yes	AT&T with two year contract	Yes	Yes
DVD Jon	No	NA	No	No
iASign Cert. (AT&T, Cingular)	Yes	AT&T, Cingular SIM, 1 SIM only	Yes	No
iASign Cert. (other ICCID)	Yes	Any Forged SIM, 1 SIM only	Yes	No
Lockdownd Patching	Yes	Any Forged SIM, Multiple SIM Support	No	No

Table 2: Activation Methods compared: SIM, firmware update and restore support.

SIM UNLOCKING METHODS

There are two SIM unlocking methods that work by fooling the iPhone into thinking that the SIM card inserted into it is the AT&T SIM card. These are:

- Super SIM Method
- Turbo SIM Method

Each of the two methods above works in a different way and has some advantages and disadvantages. The following section of the paper will discuss both of them in detail.

THE SUPER SIM METHOD

This was the world's first SIM unlock of the iPhone even though some considered it not to be a true SIM unlock method (Shmukler 2007, Sassha 2007, Kenshi 2007). The reason for calling this method a Super SIM method is because it relies on SIM programming a blank SIM card as with an old commercial product called Super SIM. It was used to clone first generation SIM cards. It was also used to combine more than one SIM card into a special high-capacity blank SIM card called "Super SIM" that enabled the user to switch between SIM cards through a special SIM management menu on the phone. The phone in this case will always see only one SIM card at a time (SuperSim 2007).

The method works by extracting the iPhone SIM card's IMSI number (issued by AT&T) and combining it with information extracted from another provider's SIM card (The user’s Telstra SIM card for example) and programming both into a third blank SIM card as shown in Figure 4 below. This is why Super SIM is sometimes referred to as a "SIM fabrication" method.

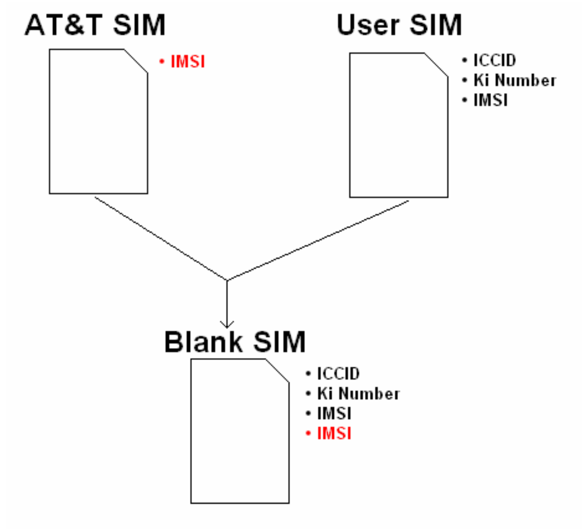


Figure 12: Super SIM Method Works.

One of the major drawbacks of this method is that the user’s SIM card has to be a first generation SIM card. This is because the method requires the decryption and extraction of the Authentication key (Ki number value) from the user's SIM card which is only possible with first generation SIM cards. So this method will not work with SIM cards by mobile phone service providers that use second generation SIM cards or providers that use 3G SIM cards.

There are many SIM card readers and programmers on the market that can be used to read SIM cards and program a blank SIM card. This paper will however focus on one of the hardware and software combinations to achieve the SIM unlock. The hardware used in this case is the Jaycar Programmer (Jaycar 2007a). Two alternative hardware programmers that were used by other iPhone hackers to successfully program a blank SIM card are Infinity USB Unlimited and Dynamite Programmer (Sassha 2007). The advantage of the Jaycar programmer over other programmers is the price and availability. It is available from Jaycar outlets and online for $49.95 Australian Dollars. The Silver Cards are also available from Jaycar for $9.95.

Jaycar SIM Card Programming

The Jaycar reader/programmer is only available in an electronics kit form and needs to be assembled. The board should also be tested according to the instructions manual that is enclosed with the kit (as on page 29 of Silicon Chip Magazine of July 2003, under heading "testing"). A blank SIM card is also needed. The appropriate blank SIM is called Silver Card which is a multi-chip smart card based on the PIC16F877 and coupled with a 24LC64 EEPROM (Jaycar 2007b).

Some additional modifications are needed to enable the Jaycar programmer to program the PIC chip part of the SIM card. These changes are as follows (Wombat et al. 2007):

- Cut the track between pins 13 and 14 on IC3.
- Cut on the side of the card that connects the switch that goes to the 10k resistor as shown by the red line in figure 5 below.
- Solder a wire from pin 13 of IC3 to the card socket side of the cut track.
- Solder a wire from pin 12 of IC3 to the mode select switch side of the cut track.

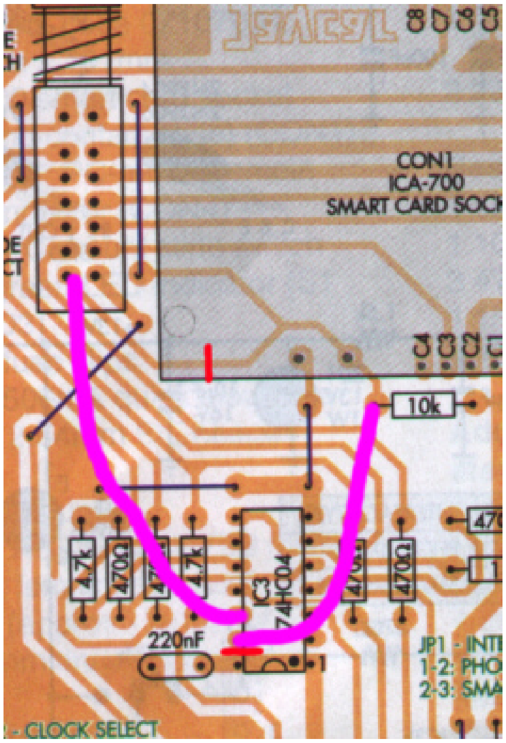


Figure 13: Hardware modifications.

The red lines on the figure above are the track cuts and the purple lines are the new connections. After assembly, the two jumpers on the board should be set as follows:

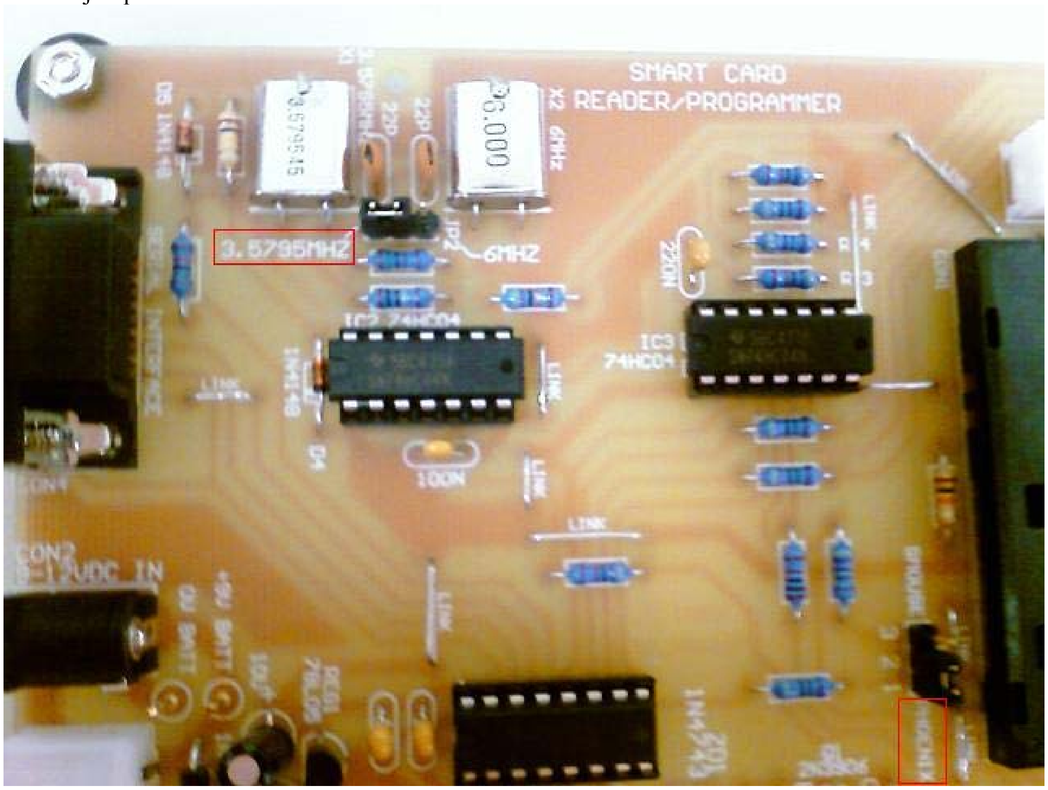


Figure 14: One jumper is on the 3.5795MHz and other is on the PHOENIX side.

Now that the hardware is ready to use, it is important to download and test it with the software needed for reading and programming the SIM card.

Testing Jaycar Programmer with Woron Scan

Woron Scan is a SIM card reading and Ki extraction software that is COM port compatible and therefore it is compatible with the Jaycar programmer (WoronScan 2007). There are some settings that need to be configured in Woron Scan before using it. They are:

- Under "Card Reader" on the top menu, "Phoenix Card" should be selected as shown below:

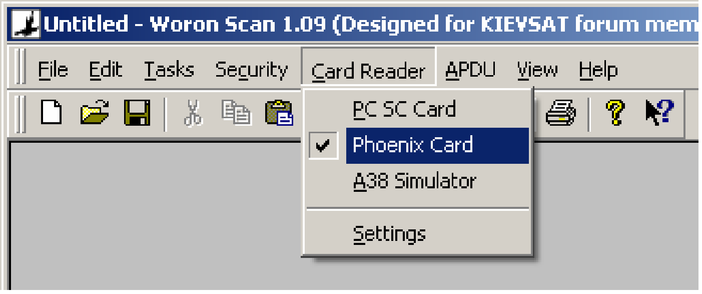
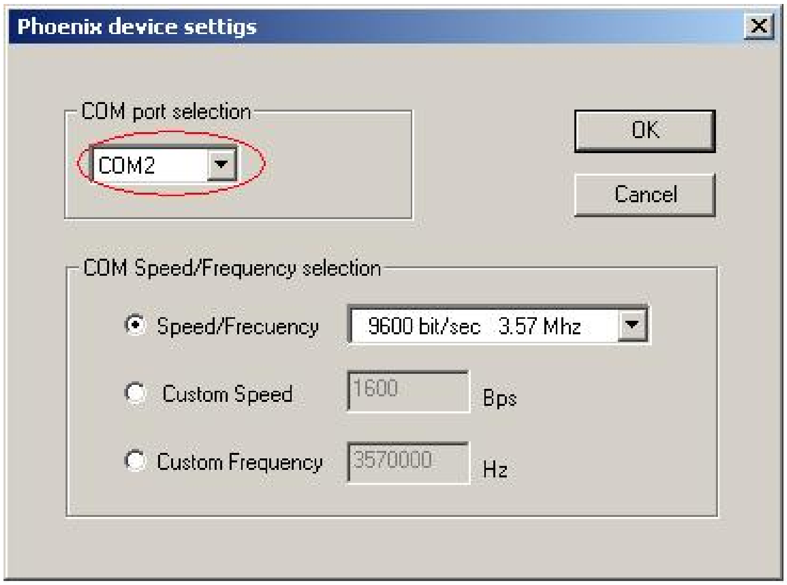

Untitled - Woron Scan 1.09 (Designed for KIEVSAT forum mem
File Edit Tasks Security Card Reader APDU View Help
PC SC Card
✓ Phoenix Card
A38 Simulator
Settings

Figure 15: Phoenix Card is selected.

- Under "Card Reader" then "Settings", the right COM port should be selected. Also, "Speed/frequency" radio button and should be set to "9600 bit/sec 3.57Mhz" from the drop down menu as show below:


Phoenix device settigs

COM port selection: COM2

COM Speed/Frequency selection

● Speed/Frecuency: 9600 bit/sec 3.57 Mhz

○ Custom Speed: 1600 Bps

○ Custom Frequency: 3570000 Hz

Figure 16: COM port where the Jaycar is connected should be selected.

Before SIM card reading, the board must be set to the correct mode. This means that the S1 switch should be on the "pressed-in" position. This is the clear switch with the green light. This switches the Jaycar programmer into the “Phoenix Mode” which is needed now to read SIM cards:

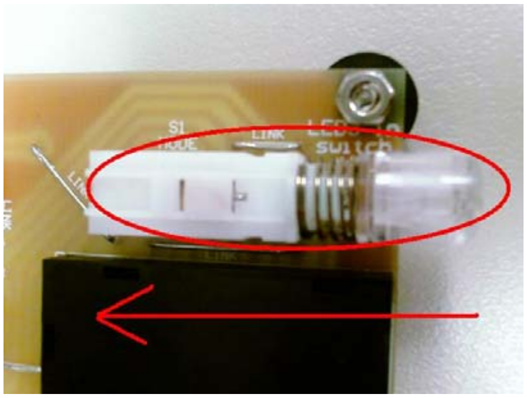


Figure 17: SI Switch Pressed.

The programmer is now ready to do the first SIM read. A first generation SIM card can now be inserted into the card reading slot for testing purposes. The contacts on the SIM card should be facing downwards. Now the "ICC" button should be pressed. If the ICCID number is displayed, this means the device is functional. If the output looks like this:

```
Communication problem... closing COM port...
The real speed is 9600..
There is a no Phoenix device or card inserted...
Communication problem... closing COM port...
```

Then there is problem with the device. Here is a list of things to consider when trouble shooting this problem:

- Make sure that the correct COM port is selected.
- Make sure that a straight-through serial cable is used to connect the programmer to the computer.
- If the cable and the port are correct then try another computer. The Jaycar programmer sometimes does NOT work with some Windows XP machines.

Reading IMSI and Extracting Ki value from SIM card

After getting the ICCID number, click on the "IMSI" button. The program should then display the SIM’s IMSI number. After that, click on the "Ki" button. It should pop up a window. In the pop-up window just click "Start" as shown in figure 10 below:

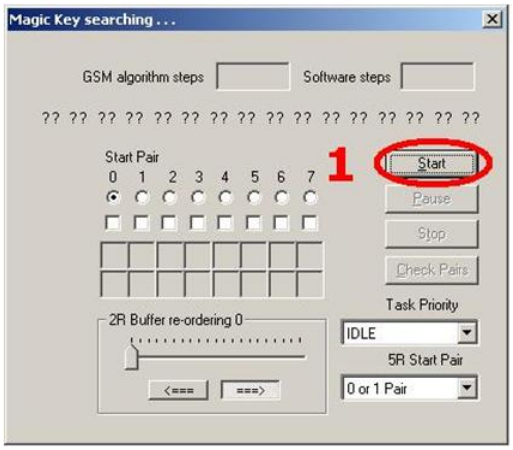
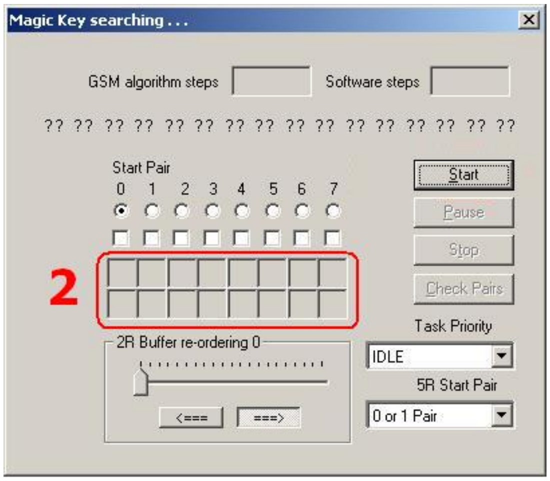


Figure 18: Press "Start" for Magic Key Searching.

Then wait for Ki extraction. This should take about 20-50 minutes. Within 10-15 minutes, some values should start popping up in the boxes shown below:



Task Priority: IDLE

5R Start Pair: 0 or 1 Pair

Figure 19: Ki number pairs should fill all the boxes in 2.

Once this operation concludes, all the values needed from the target SIM card are obtained and must be recorded. Now the AT&T SIM card should be inserted into the Jaycar programmer and the IMSI number obtained and recorded.

Super SIM Image Customization with SIM EMU

To create a Super SIM from a Blank Silver Card the following software and files are needed:

- A SIM image manipulation and programming utility. SIM EMU 6.01 will be used in this paper.
- Two customizable image files to program the PIC and EEPROM portions of the Silver Card. A ZIP file containing both images can be downloaded from the following website:
  - http://www.rapidshare.com/files/47494428/SIM_EMU_6.01_iphone_u1.rar

After installing the program, the following steps should be followed:

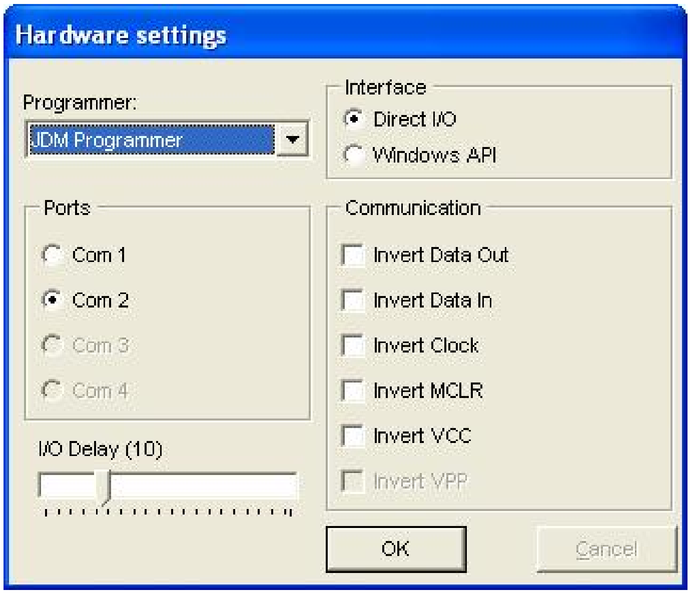
18. Click on the “Configure” tab.
19. Click on the "Read from disk" button.
20. Browse to and click on “SIM_EMU_6.01_iphone_u1.HEX”. This file is PIC programming image file contained in the ZIP file mentioned in the link above.
21. Then select and click on “SIM_EMU_6.01_iphone_u1_EP.HEX”. This file is EEPROM programming image file contained in the ZIP file mentioned in the link above.
22. In position zero "0", the data obtained from Woron Scan for the carrier SIM card (Telstra) this includes IMSI, Ki and ICCID should be entered in the corresponding fields.
23. For ADN/SMS/FDN# respectively type in 161, 15, and 4. For SMS Centre number, type in the carrier's SMS centre number including the +614 part (for Australian carriers).
24. In position "9" the IMSI from the AT&T SIM card should be typed. In PIN1, PUK1 put in all “1s” just as in position "0".
25. In "Config mode", the "Files" radio button should be selected.
26. Click on "Write to disk" button, you will be asked to save the newly created PIC and EEEPROM files, Save them under different names! For example “SIM_EMU_6.01_iphone_u1_new.HEX” and “SIM_EMU_6.01_iphone_u1_EP_new.HEX”.

This concludes the customization of the SIM images. The next step is to write the images into the blank Silver Card. A SIM card programming utility is needed for SIM card programming. The one that will be used in this paper is IC-Prog (IC-Prog 2006).

Super SIM PIC Programming with IC-Prog

Before starting to use the IC-Prog utility, it should be downloaded, installed, and configured. Therefore the following steps should be followed (Wombat et al. 2007):

- Create a directory directly under C:\ and call it IC-Prog
- Download and unzip the contents of the following files into this directory C:\IC-Prog:
  - http://www.ic-prog.com/icprog105E.zip
  - http://www.ic-prog.com/icprog_driver.zip
  - http://www.ic-prog.com/icproghh_eng.zip
- Run icprog.exe
- The following hardware settings screen should pop-up the first time IC-Prog is executed:



Hardware settings

Programmer: JDM Programmer

Interface
● Direct I/O
○ Windows API

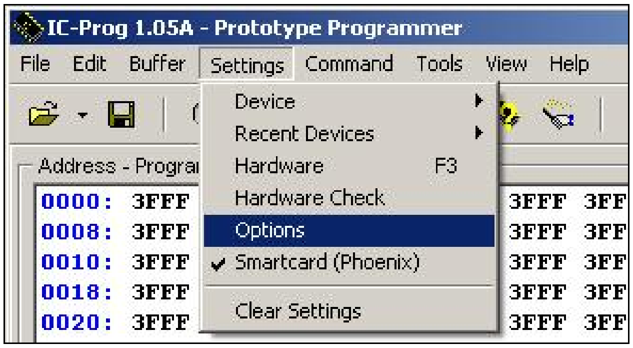
Ports
○ Com 1
● Com 2
○ Com 3
○ Com 4

Communication
□ Invert Data Out
□ Invert Data In
□ Invert Clock
□ Invert MCLR
□ Invert VCC
□ Invert VPP

I/O Delay (10)

Figure 20: Hardware Settings for IC-Prog.

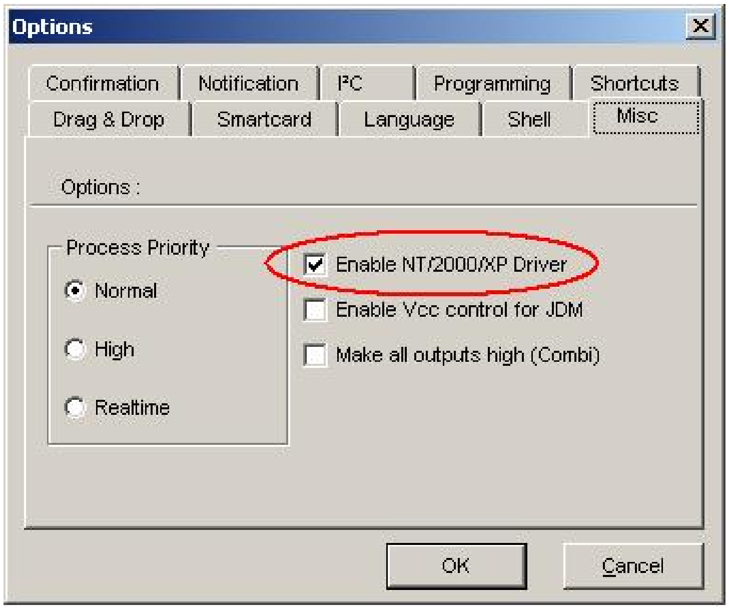
- "JDM Programmer" should be selected. Also, the appropriate COM port associated with the Jaycar programmer should be selected. The Interface should be set to "Direct I/O" and nothing should be ticked under "Communication". "OK" should be clicked next.
- Some errors should pop up at this point. Clicking "OK" should take care of them.
- Once the main program windows is shown, “Settings” tab should be selected and then options:



```
0000: 3FFF    3FFF 3FF
0008: 3FFF    3FFF 3FF
0010: 3FFF    3FFF 3FF
0018: 3FFF    3FFF 3FF
0020: 3FFF    3FFF 3FF
```

Figure 21: Select Settings then Option.

- The “Misc” tab should then be selected and under it the “Enable NT/200/XP Driver" box should be ticked as shown below:



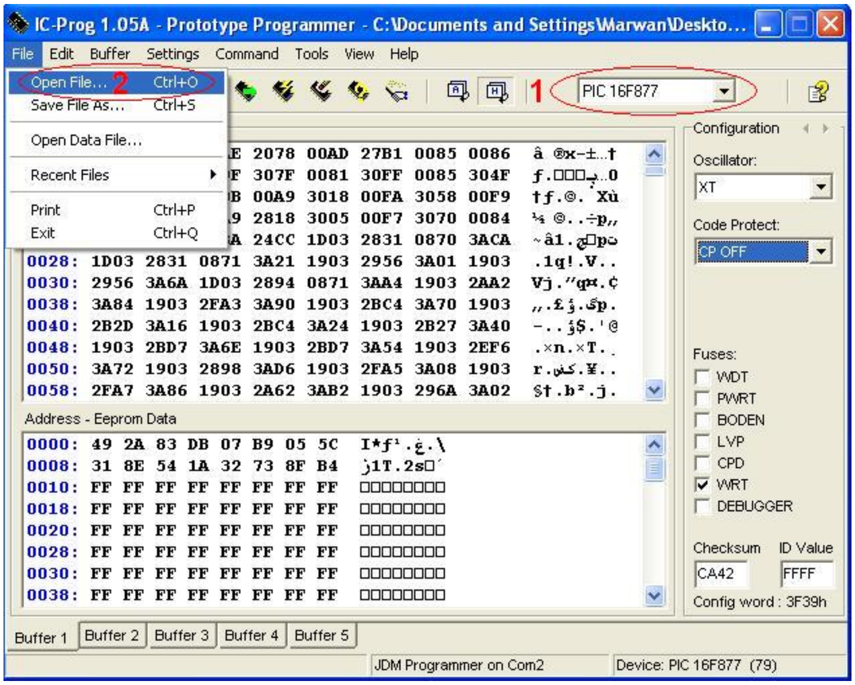
Process Priority
● Normal
○ High
○ Realtime

☑ Enable NT/2000/XP Driver
□ Enable Vcc control for JDM
□ Make all outputs high (Combi)

Figure 22: Enable NT/2000/XP Driver.

Process Priority can be left as "Normal". The Computer should be now restarted to make sure that the drivers are loaded. After that, the program should be executed again and the S1 button on the Jaycar board should be set to the "out" position. This sets the board to "PIC programming mode". To program the PIC portion of the Silver Card so the following steps should be followed (Wombat et al. 2007):

- The blank Silver card should be inserted into the Jaycar programmer.
- "PIC 16F877" should be selected from the drop down menu as shown in circle "1" in the figure below:



PIC 16F877

```
    E 2078 00AD 27B1 0085 0086   â ®x-±..†
    F 307F 0081 30FF 0085 304F   ƒ.□□□ـٻ..0
    B 00A9 3018 00FA 3058 00F9   †ƒ.©. Xù
    9 2818 3005 00F7 3070 0084   ¼ ©..÷p„
    A 24CC 1D03 2831 0870 3ACA   ~â1.ڿ□pـ
0028: 1D03 2831 0871 3A21 1903 2956 3A01 1903   .1q!.V..
0030: 2956 3A6A 1D03 2894 0871 3AA4 1903 2AA2   Vj.”q¤.¢
0038: 3A84 1903 2FA3 3A90 1903 2BC4 3A70 1903   „.£ ۆ.ڭp.
0040: 2B2D 3A16 1903 2BC4 3A24 1903 2B27 3A40   -..ۆ$.'@
0048: 1903 2BD7 3A6E 1903 2BD7 3A54 1903 2EF6   .×n.×T..
0050: 3A72 1903 2898 3AD6 1903 2FA5 3A08 1903   r.کض.¥..
0058: 2FA7 3A86 1903 2A62 3AB2 1903 296A 3A02   §†.b².j.
```

Address - Eeprom Data

```
0000: 49 2A 83 DB 07 B9 05 5C   I*ƒ¹.غ.\
0008: 31 8E 54 1A 32 73 8F B4   ژ1T.2s□´
0010: FF FF FF FF FF FF FF FF   □□□□□□□□
0018: FF FF FF FF FF FF FF FF   □□□□□□□□
0020: FF FF FF FF FF FF FF FF   □□□□□□□□
0028: FF FF FF FF FF FF FF FF   □□□□□□□□
0030: FF FF FF FF FF FF FF FF   □□□□□□□□
0038: FF FF FF FF FF FF FF FF   □□□□□□□□
```

Oscillator: XT
Code Protect: CP OFF

□ WDT
□ PWRT
□ BODEN
□ LVP
□ CPD
☑ WRT
□ DEBUGGER

Checksum: CA42
ID Value: FFFF
Config word : 3F39h

JDM Programmer on Com2
Device: PIC 16F877 (79)

Figure 23: Setting up IC-Prog for PIC programming (1) and loading a PIC file (2)

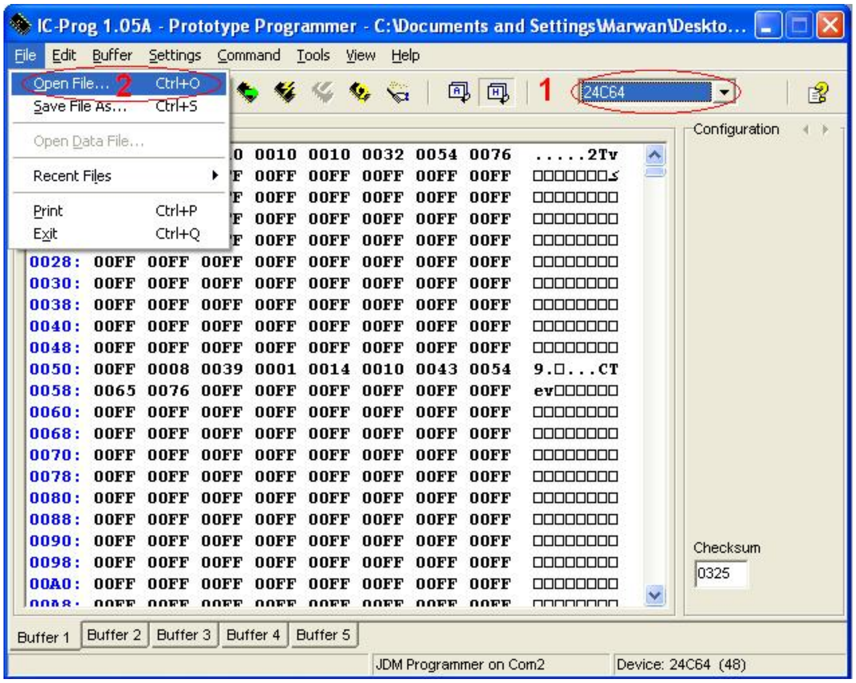
- The PIC file should now be opened by clicking "File" and then selecting "Open File" (as in circle 2 in Figure 15) and selecting "SIM_EMU_6.01_iphone_u1_new.HEX" created in the SIM image file customization steps discussed earlier.
- "Code Protect" drop down menu should be set to "CP OFF" which turns off copy protection.
- Function Key "F5" should now be pressed to start programming the PIC portion of the Silver Card. This process should take around 5-10 minutes.

This concludes the PIC programming part of the SIM card creation. The next step is program the EEPROM portion of the blank SIM Card.

Super SIM EEPROM Programming with IC-Prog

The IC-Prog utility should now be configured to program the EEPROM part of the Silver Card. The following steps should be followed (Wombat et al. 2007):

- In the drop-down menu, "24C64" should be selected as shown in circle "1" below:



```
0 0010 0010 0032 0054 0076   .....2Tv
F 00FF 00FF 00FF 00FF 00FF   □□□□□□□ऽ
F 00FF 00FF 00FF 00FF 00FF   □□□□□□□□
F 00FF 00FF 00FF 00FF 00FF   □□□□□□□□
F 00FF 00FF 00FF 00FF 00FF   □□□□□□□□
0028: 00FF 00FF 00FF 00FF 00FF 00FF 00FF 00FF   □□□□□□□□
0030: 00FF 00FF 00FF 00FF 00FF 00FF 00FF 00FF   □□□□□□□□
0038: 00FF 00FF 00FF 00FF 00FF 00FF 00FF 00FF   □□□□□□□□
0040: 00FF 00FF 00FF 00FF 00FF 00FF 00FF 00FF   □□□□□□□□
0048: 00FF 00FF 00FF 00FF 00FF 00FF 00FF 00FF   □□□□□□□□
0050: 00FF 0008 0039 0001 0014 0010 0043 0054   9.□...CT
0058: 0065 0076 00FF 00FF 00FF 00FF 00FF 00FF   ev□□□□□□
0060: 00FF 00FF 00FF 00FF 00FF 00FF 00FF 00FF   □□□□□□□□
0068: 00FF 00FF 00FF 00FF 00FF 00FF 00FF 00FF   □□□□□□□□
0070: 00FF 00FF 00FF 00FF 00FF 00FF 00FF 00FF   □□□□□□□□
0078: 00FF 00FF 00FF 00FF 00FF 00FF 00FF 00FF   □□□□□□□□
0080: 00FF 00FF 00FF 00FF 00FF 00FF 00FF 00FF   □□□□□□□□
0088: 00FF 00FF 00FF 00FF 00FF 00FF 00FF 00FF   □□□□□□□□
0090: 00FF 00FF 00FF 00FF 00FF 00FF 00FF 00FF   □□□□□□□□
0098: 00FF 00FF 00FF 00FF 00FF 00FF 00FF 00FF   □□□□□□□□
00A0: 00FF 00FF 00FF 00FF 00FF 00FF 00FF 00FF   □□□□□□□□
00A8: 00FF 00FF 00FF 00FF 00FF 00FF 00FF 00FF   □□□□□□□□
```

Checksum 0325

JDM Programmer on Com2   Device: 24C64 (48)

Figure 24: Setting up IC-Prog to program the EEPROM portion of the SIM card

- The EEPROM file should now be opened by clicking "File" and then selecting "Open File" (as shown in circle two in Figure 16) and selecting "SIM_EMU_6.01_iphone_u1_EP.HEX" created in the SIM image file customization steps discussed earlier.
- Function Key "F5" should now be pressed to start programming the EEPROM portion of the Silver Card. This process should take around 5-10 minutes.

This concludes the EEPROM programming part of the SIM card creation. The Silver card is ready now to be inserted into the iPhone. After inserting the SIM card into the iPhone, the phone should display that the SIM is locked and will ask for a SIM PIN number to activate the SIM card. The number that should be entered is "1111".

THE TURBO SIM METHOD

Turbo SIM is a microchip based device that is developed by the Czech Republican company Bladox (Bladox 2007). It is about the size of a SIM card but it is less than one millimetre in thickness. The device is designed to be placed between the Phone and a SIM card. It is programmable with a SIM Toolkit wireless Application Programming Interface (API). The device can be programmed to intercept and modify communications from the phone to the SIM card and vice versa.

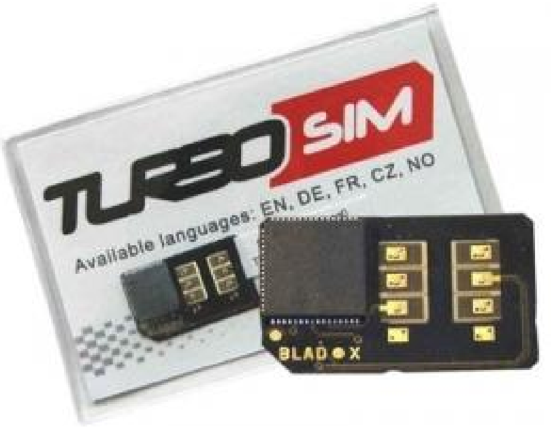


Figure 25: Turbo SIM

Turbo SIM can be used to fool the iPhone into thinking that the SIM card it is communicating with is actually the AT&T SIM card associated with the iPhone. The Turbo SIM does this by intercepting specific inquires from the iPhone about the SIM card's IMSI and providing the previously programmed AT&T SIM card's IMSI instead of the actual IMSI from the SIM card placed behind the Turbo SIM. This effectively makes iPhone compatible with any GSM SIM card inserted behind the Turbo SIM.

Turbo SIM Preparation and Programming

In order to program the Turbo SIM to intercept specific IMSI requests from the iPhone, an AT&T SIM card needs to be cut and placed behind the Turbo SIM and both inserted into a jailbroken iPhone. Then the following two files should be uploaded into the iPhone (Farnoud 2007):

- **applesaft.trb**: The image file that needs to be uploaded to the Turbo SIM's internal memory. The file can be downloaded from Bladox at: http://www.bladox.com/pub/applesaft-0.92.tar.gz
- **turbo-app**: The upload application that can be run on the iPhone to upload "applesaft.trb" into the Turbo SIM's internal memory. It can be downloaded from: http://www.gofilego.com/?fileid=71aef6d5c92b32b596cbf6bec73da7541ee37ae8

After the files are uploaded, the turbo-app needs to be executed on the iPhone. This requires changing the following file on the iPhone: "/System/Library/LaunchDaemons/com.apple.CommCenter.plist" and adding the following line: "<key>Disabled</key><true/>" after the following tag in the file (Farnoud 2007):

```
<key>OnDemand</key>
<false/>
```

Permissions on turbo-app and on applesaft.trb need to be changed to 775. Then turbo-app can be executed on the iPhone as follows: */turbo-app /applesaft.trb*

The applesaft.trb is now uploaded to the iPhone and can be executed by going to Settings -> Phone -> SIM Applications -> Apple Saft and then clicking SET. This copies the IMSI number of the AT&T SIM card to the the Turbo SIM. The modified file: "/System/Library/LaunchDaemons/com.apple.CommCenter.plist" can now be returned to its normal state by removing the added line of code. Any SIM card can now be cut and placed behind the Turbo SIM and the iPhone will not be able to view its real ICCID.

The main advantage of the Turbo SIM method over Super SIM is that any GSM SIM card can be placed behind the Turbo SIM therefore it is not limited to first generation SIM cards as with Super SIM. Also, the Turbo SIM method is easier to follow than the Super SIM method and fewer things can go wrong during the process when compared to Super SIM. The disadvantages of Turbo SIM include the high price and scarce availability of the Turbo SIM device. The Turbo SIM retail price is $159 Australian Dollars but because of high demand associated with the iPhone hack, the manufacturer and suppliers ran out of it (Votech 2007). Another disadvantage of Turbo SIM is that it is fragile. Many iPhone users ended up damaging their Turbo SIM by trying to fit it within iPhone's SIM card tray (MetalRat 2007). Another issue with the Turbo SIM is the contacts between the Turbo SIM and the SIM card placed behind it sometimes don't touch. This could be because of a physical problem with the Turbo SIM device or the SIM card placed behind it or a combination of both.

SOFTWARE SIM UNLOCKING

Super SIM and Turbo SIM unlocking methods revolve around the fabrication of a SIM card. The software unlocking methods however achieve SIM unlocking by modifying the base band software on the iPhone itself. This was not thought to be possible by the hacking community until a commercial website iPhoneSIMFree.com started selling a software based unlocking solution through their re-sellers. The hacking team behind the free software unlock then reverse engineered the commercial software and discovered that it works by programming (flashing) the base band software of the iPhone. After that, a free software application called AnySIM was developed to unlock the iPhone. The disadvantages of this type of unlocking are as follows: First, the software only works with a specific version of iPhone's phone firmware and modem firmware, namely phone firmware version: 1.0.2 (1c28) and modem firmware version: 03.14.08_G. The second disadvantage is that using this unapproved software on the iPhone voids Apple's warranty. Also, updating the iPhone to firmware version 1.1.1 and beyond may render the iPhone useless (brick the iPhone) (Miller 2007).

ADVANCED TECHNIQUES

Other third party software beyond SIM unlocking can also be installed to the iPhone even though it is considered unapproved software and can void the warranty and brick the iPhone (Murph 2007). This can be done in many ways; one of these ways is through using software called iBrikr which enables ring tones and applications including AnySIM to be installed on the iPhone (True 2007).

Unlocking the iPhone with AnySIM based SIM unlocking can enable the iPhone to be used with Multi-SIM adapters such as Hyper Card (MagicSIM 2007). Multi-SIM adapters allow two SIM cards to be cut down in size by using a special tool and they are then inserted into a special SIM-card-shaped adapter that can be inserted into the iPhone.

The iPhone can then be used with two SIM cards at the same time; one SIM card on stand-by and one active SIM card. Inserting the card into the iPhone can be difficult due to the thickness of the adapter itself, the thickness of the two SIM cards inserted into it and the thickness of a microchip that sticks out of the adapter as shown in the circle marked 1 in the figure below:

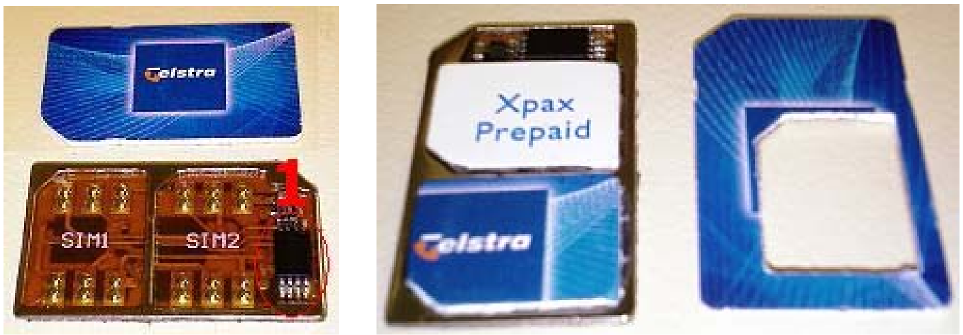


Figure 26: Hyper-Card and Telstra SIM card before and after SIM cutting and placement with another SIM card.

The adapter adds a SIM management screen to the iPhone that enables SIM card selection and other options to be selected such as setting the a number for each SIM or an ID for each for easy maintenance.

UNBRICKING THE IPHONE

In electronics, the term bricked describes a device that cannot function in any capacity such as an iPhone with a damaged firmware. The iPhone can be bricked by disrupting a firmware upgrade or corrupting a system file or some other damage to the Operating System (OS) software. In this case, the iPhone can be unbricked by using the restore function from within the iTunes software within Windows XP. The following are the steps to follow (Batten 2007):

- Download the desired iPhone update file from Apple.

- Place the file under the following directory in Windows: **Documents and Settings\<User Name>\Application Data\Apple Computer\iTunes\iPhone Software Updates**
- Hold the “shift” key while clicking the iPhone "Restore" button in iTunes.
- Select the firmware file to use from the dialog box.
- The restore operation should take a few minutes after which the iPhone will be reset to factory new status.

The iPhone may also become bricked if it is updated to firmware version 1.1.1 after being activated via means other than the iTunes-AT&T activation or SIM unlocked via the AnySIM software update (Miller 2007). In this case, the unbricking process is more complex but unbricking guides can still be found on the Internet (iPhone-Elite 2007).

CONCLUSION AND CONSIDRATIONS

Warranty issues with iPhone activation and unlocking should be considered when attempting any of the hacks on the iPhone. SIM fabrication methods are the only methods that do not void the warranty because they do not change anything in the iPhone but rather, they modify SIM cards to work with the iPhone. Some activation methods such as the iASign and the patching method are easily reversible by restoring the iPhone to factory settings from iTunes thus not voiding the warranty. Hardware modifications such as the Geohot hardware re-wiring method made famous on the Internet should never be attempted as they will definitely void the iPhone’s warranty (Geohot 2007).

REFERENCES

Al-Zarouni, M. (2007) iPhone Unlocked for All SIMs?, URL http://www.mysecured.com/?p=159, Accessed 17 September 2007

Apple (2007a) Apple - iPhone - Features - Voicemail, URL http://www.apple.com/iphone/features/index.html#voicemail, Accessed 11 October 2007

Apple (2007b) Apple - iPhone - High Technology, URL http://www.apple.com/iphone/technology/, Accessed 18 September 2007

Batten, A. (2007) Is there a way to restore my iPhone with a selected version of iPhone firmware?, URL http://www.iphonefaq.org/archives/97285, Accessed 23 October 2007

Bladox (2007) BLADOX, URL http://www.bladox.com/, Accessed 16 October 2007

Cauley, L. (2007) AT&T eager to wield its iWeapon, URL http://www.usatoday.com/tech/wireless/2007-05-21-at&t-iphone_N.htm, Accessed 24 October 2007

DevWiki (2007) How Activation Works - The iPhone Dev Wiki, URL http://iphone.fiveforty.net/wiki/index.php/How_Activation_Works, Accessed 10 October 2007

Farnoud, H. (2007) iPhone Unlocked, URL http://hadi.wordpress.com/2007/08/14/iphone-unlocked/, Accessed 23 October 2007

Geohot (2007) Finding JTAG on the iPhone: FULL HARDWARE UNLOCK OF IPHONE DONE, URL http://iphonejtag.blogspot.com/2007/08/full-hardware-unlock-of-iphone-done.html, Accessed 23 October 2007

HTIP (2007) Hack the iPhone - Using non-stock SIMs in the iPhone on Windows, URL http://www.hacktheiphone.net/iphone_using_cingular_for_windows.html, Accessed 10 October 2007

IC-Prog (2006) IC-Prog Prototype Programmer, URL http://www.ic-prog.com/, Accessed 16 October 2007

iPhone-Elite (2007) DowngradingBaseband - iphone-elite - Google Code, URL http://code.google.com/p/iphone-elite/wiki/DowngradingBaseband, Accessed 23 October 2007

Jaycar (2007a) Full Function Smart Card Reader / Programmer Kit URL http://www.jaycar.com.au/productView.asp?ID=KC5361, Accessed 15 October 2007

Jaycar (2007b) Silver Wafer Card, URL http://www.jaycar.com.au/productView.asp?ID=ZZ8810, Accessed 15 October 2007

Johansen, J. L. (2007) iPhone Independence Day, URL http://nanocr.eu/2007/07/03/iphone-without-att/, Accessed 17 September 2007

Johnston, M. (2007) anySIM Released: Free GUI iPhone Unlock, URL http://www.iphonealley.com/news/anysim-released-free-gui-iphone-unlock, Accessed 30 October 2007

Kenshi (2007) iPhone making calls on Australia's Telstra (iPhone + hack + iActivator + ozbimmer), URL http://tech.commongate.com/post/iPhone_making_calls_on_Australia_s_Telstra, Accessed 17 September 2007

MagicSIM (2007) Hyper-Card for iPhone, URL http://hyper-card.com/home/english/main.htm, Accessed 23 October 2007

MetalRat (2007) A Muppet's Guide to TurboSIM - Hackint0sh, URL http://www.hackint0sh.org/forum/showthread.php?t=2663, Accessed 23 October 2007

Miller, P. (2007) iPhone update: facts and fiction, URL http://www.engadgetmobile.com/2007/09/28/iphone-update-facts-and-fiction/, Accessed 23 October 2007

Murph, D. (2007) Apple finally weighs in on iPhone hacks, unlocking, URL http://www.engadget.com/2007/09/24/apple-finally-weighs-in-on-iphone-hacks-unlocking/, Accessed 23 October 2007

Sadun, E. (2007) iPhone + Disposable Cellphone + Prepaid Cards + New Activation Tool = Holy Cow, URL http://www.tuaw.com/2007/07/18/iphone-disposable-cellphone-prepaid-cards-new-activation-t/, Accessed 17 September 2007

Sassha (2007) Tutorial: "Unlock" your iPhone with SuperSim - Hackint0sh, URL http://www.hackint0sh.org/forum/showthread.php?t=2215, Accessed 17 September 2007

Shmukler, C. (2007) Apple iPhone Unlocked for Use in Europe, URL http://www.iphonefaq.org/archives/97228, Accessed 15 October 2007

SuperSim (2007) Super SIM 16 in 1, URL http://www.nowgsm.com/supersim.htm, Accessed 15 October 2007

TMHGIH (2007) The Most Hyped Gadget In History, URL http://www.tmhgih.com/, Accessed 10 September 2007

True, N. (2007) iBrickr: Easy iPhone ringtone / app management for Windows, URL http://cre.ations.net/creation/ibrickr, Accessed 23 October 2007

ValeraVi (2007) Site of ValeraVi - V_KLay and patches for Siemens mobile phones, URL http://www.vi-soft.com.ua/index_e.htm, Accessed 11 October 2007

Votech (2007) Votech - Turbo SIM Status Updates, URL http://www.votech.com.au/bladox_updates.php, Accessed 23 October 2007

Wombat, TheGuide, Secured & freeproductions (2007) Jaycar Kit - Hackint0sh, URL http://www.hackint0sh.org/forum/showthread.php?t=2805, Accessed 25 October 2007

WoronScan (2007) Woron Scan Download, URL http://www.kinforce.com/down/kinforce/supersim/ws109.zip, Accessed 15 October 2007

COPYRIGHT