International Journal of Scientific & Engineering Research, Volume 3, Issue 8, August-2012
ISSN 2229-5518

Counter Strike: Prompt Gaming Time on Android and iPhone

Himanshu Srivastava, Tanupriya Choudhury, Vasudha Vashisht

Abstract-- Mobile phones are becoming exotic for mankind and did their respective job with ably, it also abridge form of laptop and palmtop also. We always extol games, since our childhood. Nowadays, mobile phones are indispensable for everyone, it amuse as well as the medium for communication. In this paper, we target to counter strike, stimulating gaming; and make it compatible to iPhone (and android phones). With the introduction of Apple's iOS and Google's Android operating systems, the sales of smart-phones have exploded. These smart-phones have become powerful devices that are basically miniature versions of personal computers. However, the growing popularity and sophistication of smart-phones have also increased concerns about the privacy of users who operate these devices. These concerns have been exacerbated by the fact that it has become increasingly easy for users to install and execute third-party applications. In this paper, we study the privacy threats that applications, written for Apple's iOS, pose to users. To this end, we present that allow us to analyze programs for possible leaks of sensitive information from a mobile device to third parties. This experiment show that, with the exception of a few bad apples, most applications respect personal identifiable information stored on user's devices. This is even true for applications that are hosted on an unofficial repository (Cydia[17]) and that only run on jail-broken phones The proposed system will enlighten of jailbreak of iPhone and make its APTickets (are the new type of SHSH blobs) protocol compatible to Telnet Protocol so the file transfer would be easy without any forbidden rule provided by apple corporation, Address space layout randomization (ASLR) which involves randomly arranging the positions of key data areas, usually including the base of the executable and position of libraries, heap, and stack, in a process's address space. This includes some changes in iphone and one more thing the portable counter-strike which is powered by unity technology being run by installous[18] on the iPhone, and in android it is quite simple in this manner, because it doesn't require any jail breaking techniques but should be compatible to run the game. In this proposed system, we firstly go through all the tactics of jail breaking regarding to the iphone and then move on the android, it's quite artlessness regarding to the android phone comparatively to the iPhone to run counter strike. The proposed system is favorable to both, either by jail-breaking through reverse engineering or by installous[18] software, in this paper, It will demonstrate both the tactics reverse engineering as well as installous[18], inclusively.

Index Terms—APTicket, Address space layout randomization, Android, Counter-Strike, installous, iPhone, jail-break, Reverse engineering.

1. INTRODUCTION

Mobile phones have rapidly evolved over the last years. The latest generations of smart phones are basically miniature versions of personal computers; they offer not only the possibility to make phone calls and to send messages, but they are a communication and entertainment platform for users to surf the web, send emails, and play games. Mobile phones are also ubiquitous, and allow anywhere, anytime access to information. In the second quarter of 2010 alone, more than 300 million devices were sold worldwide [3]. Since the introduction of Apple's iOS and the Android operating systems, smart-phone sales have significantly increased.

The ability to run third-party code on a mobile through reverse engineering this is going to be crazy.

- *Himanshu Srivastava is currently pursuing Bachlor degree program in computer science engineering in Gautam Buddha Technical University, India, PH-09453037414, himuvini1990@gmail.com*
- *Tanupriya Choudhury is currently pursuing Doctrate degree program from Jagannath University(India) working in computer science engineering in Lingaya's University, India, PH-09711938087. tanupriya86@gmail.com*
- *Vasudha Vashisht is currently pursuing Doctrate degree program from Lingaya's University(India) working in computer science engineering in Lingaya's University,India,PH-09999505309, ervasudha@gmail.com*

Well, technology is moving gradually in the field of game, Today the structure and the presentation of virtual games are rapidly moving in a form where none other than any technology are moving, in those, one among them is counter strike(Game). In this proposed system, it includes, check all of its security features which have some certain chronicle verification i.e. Bootloader verification which includes Signed firmware, Signed kernel, Signed Applications and another one is installed from the app store which is signed by Apple for everything, which provides a platform to run that software on iPhone. In this proposed system, I am going to show counter strike fully functioned game, counter strike on iPhone and Android phone, this is done only by jail breaking through reverse engineering. Let's have a look toward jailbreak, In order to run unofficial or unapproved third-party applications on these mobile computing platforms, a user needs to jailbreak the device by modifying the host system software. Depending on the tool used to accomplish the jailbreak, the process could entail injecting code into the host system software while it remains on the device, or alternatively extracting the host system software to a computer to make the necessary modification and then subsequently reloading the altered host system software back to the device. Once a device is jail-broken, the user can run non-

digitally signed code, a capability that was technically forbidden on stock devices. This allows the installation of numerous third-party applications that independent software developers create. These Applications may have advanced capabilities or grant the user administrative access to the device, allowing customization to both the form and function of the system software. Jailbreak does not slow down your device or use extra battery, and you can still use all your existing apps and buy new ones from the App Store.

2. APPLICATION SECURITY PROCESS

Apparently, all the process which intakes in iPhone, has some certain security policy, according to which they can run the kernel files which handles process in a series. Here the architecture of security which is followed by and works likewise.

Code signing
- All applications (apps) must be signed by Apple.
- Signatures stored in mach-o header section.
- Check implemented in kernel as an enhanced execv()

Sandbox
- Applications run as "mobile".
- Chroot sandbox ostensibly restricts apps to their own data.
- Can't alter the OS or other apps.

Due to these, third party software is unable to run in iPhone but with reverse engineering, the precursor of iPhone will more easily handle. In addition, counter-strike game console have its own server which might occur some problem at run time so it also have some modification to run the server at gaming time. It would updated by the following command.

HldsUpdateTool.exe -command update -game "Counter-Strike Source" –dir
"C:\Program Files\Valve\HLServer\srcds.exe" -console -game cstrike -autoupdate +maxplayers 20 +map cs_italy
srcds.exe -console -game cstrike -autoupdate +maxplayers 20 +map cs_italy

3. PROCESS AND STEPS WITH REVERSE ENGINEERING

Counter-strike, the game itself represent all about itself. It is ubiquitous and popular as a game the game kept people hooked to it by never being short of action, players never knowing when an enemy may pop out at you. Running around the corner and getting shot down by an enemy, sneaking up on an enemy stealth like and brining them down with a knife and laughing at them after wards. The process by which it would be compatible to run upon iPhone and Android is Address space layout randomization (ASLR), comex the developer of Spirit, ecid, APTicket.

1.1 Part 1-

iOS Restore Process or SHSH(APTicket)

During restore an APTicket request is sent to Apple gs.apple.com
- Connection is plaintext HTTP.
- APTicket request contains hashes for each firmware file 6

POST /TSS/controller?action=2 HTTP/1.1 Accept: */*
Cache-Control: no-cache
Content-type: text/xml; charset="utf-8"
User-Agent: InetURL/1.0
Content-Length: 12345
Host: gs.apple.com (here comes the Plist request file)

Response from server looks like

HTTP/1.1 200 OK
Date: Sun, 15 Aug 2010 19:25:18 GMT
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.4; JBoss-4.0.5.GA (build: CVSTag=Branch_4_0
date=200610162339)/Tomcat-5.5
Content-Type: text/html
Content-Length: 123456
MS-Author-Via: DAV
STATUS=0&MESSAGE=SUCCESS&REQUEST_STRING=(here comes the requested SHSH file)

Following status responses are known

STATUS=0&MESSAGE=SUCCESS
STATUS=94&MESSAGE=This device isn't eligible for the requested build.
STATUS=100&MESSAGE=An internal error occurred.
STATUS=511&MESSAGE=No data in the request
STATUS=551&MESSAGE=Error occured while importing config packet with cpsn:
STATUS=5000&MESSAGE=Invalid Option!

3.2 Part2-

ASLR (Address Space Layout Randomization)

Address space layout randomization (ASLR) is a computer security method which involves randomly arranging the positions of key data areas, usually including the base of the executable and position of libraries, heap, and stack, in a process's address space. Address space randomization is more effective when more entropy is present in the random offsets. Entropy is increased by either raising the amount of virtual memory area space over which the randomization occurs or reducing the period over which the randomization occurs. The period is typically implemented as small as possible, so most systems must increase VMA space randomization. Randomly slides dynamic library cache, main binary and dyld(Dynamic Link Loader) is:

dyld_shared_cache randomness = ~4200 different positions
main binary = 256 different positions (if PIE binary)
dyld binary = 256 different positions (if main binary is PIE)

Main binary can only be slide if it is PIE (Position Independent Executables) compiled. ASLR can be easily bypassed within a launchdaemon configuration unfortunately now public due to corona.

A sample form to bypass ASLR in an untether

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
   <key>Label</key>
<string>jb</string>
<key>ProgramArguments</key>
<array>
      <string>/usr/sbin/corona</string>
<string>-f</string>
<string>racoon-exploit.conf</string>
   </array>
<key>WorkingDirectory</key>
<string>/usr/share/corona/</string>
<key>RunAtLoad</key>
<true/>
<key>LaunchOnlyOnce</key>
<true/>
<key>DisableAslr</key>
<true/>
</dict>
</plist>
```

3.3 Part3-

Partial Code-signing Vulnerability

In iOS 4.x jailbreaks the method of choice to launch untether exploits, when a mach-o is loaded the kernel will load it as is A possible signature will be registered, missing signature is okay until a not signed executable page is accessed. The dyld (Dynamic link loader) is tricked with malformed mach-o data structures to execute code. When /var/db/.launchd_use_gmalloc exists launched will re-exec itself with injected library injected library /usr/lib/libgmalloc.

dylib is a malicious lib that tricks dyld, function interposing is used to redirect execution of the launched binary into code gadgets.

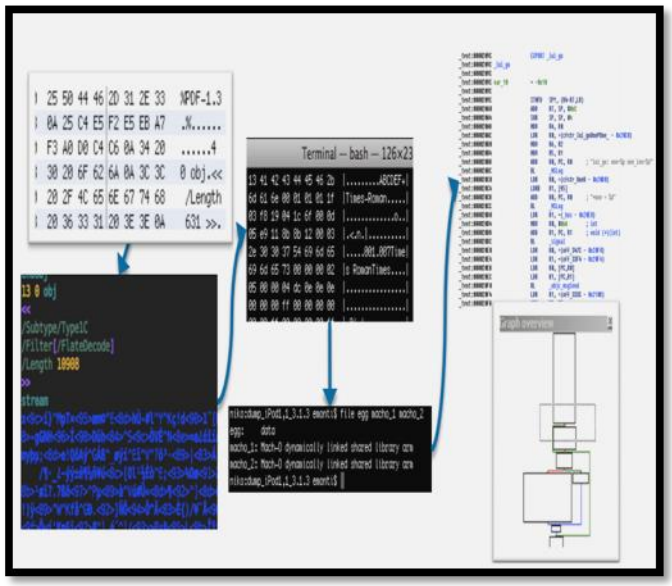

Fig1- figure illustrate Reversing the Exploit Binaries (pre-source)

3.4 Part4-

Kernel Heap Allocator Changes

XNU has many different kernel heap allocation functions this is just a small extract around _MALLOC and friends' iOS 5 brings changes to _MALLOC and kalloc more in my upcoming paper about the kernel heap.

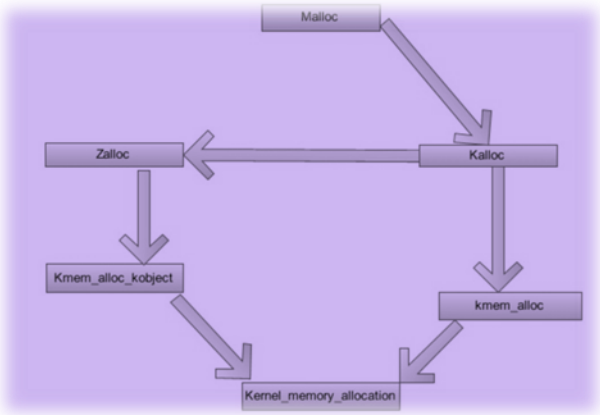

Fig2-model diagram of kernel heap allocator change (extractor)

kalloc() is a wrapper around zalloc() and kmem_alloc() for small requests zalloc() is used for bigger requests kmem_alloc() is used kalloc() registers several zones with names like kalloc.*

kalloc.* zones exists for different powers of smallest zone is for 16 byte long memory blocks every memory block is aligned on its own size. In the below code, malloc() function defines, where kalloc_noblock (memory size) is tricked with memory header, malloc() function, here simply illustrate that that detect size, if it overflow then it shows detection, otherwise it will return to the header.

A Sample form for kernel heap allocator change

```
void *_MALLOC(size_t size, int type, int flags)
{
   struct _mhead   *hdr;
   size_t memsize = sizeof (*hdr) + size;
   int overflow = memsize < size ? 1 : 0;
   ...
   if (flags & M_NOWAIT) {
      if (overflow)
         return (NULL);
      hdr = (void *)kalloc_noblock(memsize);
   } else {
      if (overflow)
      panic("_MALLOC: overflow detected, size %llu",
size);
      hdr = (void *)kalloc(memsize);
      ...
   }
   ...
   hdr->mlen = memsize;
return  (hdr->dat);
}
```

3.5 Part5-

Activating KDP for iPhone

There is no public bootrom exploit but i can trick an already exploited kernel I have to fake boot arguments, patch some data and call several initialize functions. Find kalloc() in kernel binary call it to allocate some memory write debug=8 boot argument into this memory. Find PE_boot_args() in kernel binary patch it to return a pointer to our fake boot arguments. The below table, shows that the Reverse engineering code which I got, while doing this stuff.

80240084	_PE_boot_args	; CODE XREF: 80016886p
80240084		; j__PE_boot_argsj
80240084 01 48	LDR	R0, =dword_802F52F8
80240086 00 6F	LDR	R0, [R0,#(dword_802F5368 - 0x802F52F8)]
80240088 38 30	ADDS	R0, #0x38
8024008A 70 47	BX	LR

Finally find kdp_init() in kernel binary call it to initialize the serial KDP.

This is all the reverse code and fundamental steps by which the jailbroken of iPhone is possible but it is applied only in iOS5.0x series only because apple always make changes in their buffer memory and also in ASLR so it is quite tough for the attacker to run some third party application in their own iPhone. To overcome this problem, greenpoisi0n is most trusted software package by which jailbreak would much simpler.

4. JAILBRAKING WITH SOFTWARE PACKAGE

Jailbreak at its initial time was much tough and it is harder to jailbreak the iPhone and iPad to access the authentication, but with the help of Greenpoisi0n, it is much easier to access the authentication of the third party software. Greenpois0n is an untethered jailbreak tool to jailbreak iPhone 3GS, iPhone 4 GSM, iPhone 4 CDMA, iPod touch 2G, iPod touch 3G, iPod touch 4G. It uses mainly Limera1n Boot-ROM exploit (originally SHAtter Boot-ROM exploit),for untether (ability to reboot device without connecting it to a computer and re-execute Jailbreak) user-land (software) exploits named "Packet filter kernel exploit" for 3.2.2-4.1, and HFS Legacy Volume Name Stack Buffer Overflow exploit on 4.2.1-4.2.6. Greenpois0n was originally meant to jailbreak iOS 3.2 on the iPad. After Spirit's user-land jailbreak by the iPhone Dev Team member Comex, capable of jailbreaking the iPad's firmware 3.2 and iOS 3.1.2 and 3.1.3. The Chronic Dev Team has continued working on Greenpois0n, even after iOS 3.2.1 was released for the iPad and iOS 4.0/4.1 for the iPhone and iPod touch.

4.1 Step 1-

Launch greenpoisi0n and do jailbreak

At the very first step, go to the Greenpoisi0n[32] website and download the software according to your operating system and compatibility of your RAM and processor. After successfully installation of the greenpoisi0n software, just install it as a recommended permission. After successfully installation of the software, it will ask for to connect the iPhone to your personal computer via data cable, as illustrated figure below.

Fig 3- demonstration of jail breaking

After that, click on prepare to jailbreak button, then follow the instruction likewise:

4 Press and hold the sleep button for two second.
5 Continuing holding sleep; press and hold home button for 10 second.
6 Release sleep button; continue holding home button for 15 second.
7 Then after, switch off the iPhone and let the greenpoisi0n software to work itself.
8 After then click on the button, prepare jailbreak.
9 It will follow some Linux coding, which will run until the logo of apple not converted into greenpoisi0n logo.

By doing, all these steps finally, close the window of greenpoisi0n which is running in your personal computer, and this is all done with jailbreak with your iPhone.

4.2 Step 2-

Loader loads Cydia

Cydia[17] is a software application for iOS that enables a user to find and install software packages (including apps, interface customizations, and system extensions) on a jailbroken iPhone, iPod Touch or iPad. Cydia is the main independent third-party digital distribution platform for software on iOS. Many of the software packages available through Cydia are free, and it also includes several hundred packages for sale through the Cydia Store payment system with a commission setup similar to the App Store. Most of these packages focus on providing customizations and modifications (often called "tweaks") that can only run on jailbroken devices (since the App Store is limited to distributing self-contained apps). Cydia is a graphical front end to Advanced Packaging Tool (APT) and the dpkg package management system, which means that the packages available in Cydia[17] are provided by a decentralized system of repositories (also called sources) that list these packages. To download the package tools from cydia[17], user has to firstly install cydia in their own iPhone. Let me show you the steps, which governs the installation process of cydia and it's free third part package tools.

a. Firstly go to your iPhone manager setting tab and click for source tab.
b. After that go for add tab which is located in your iPhone's topmost left corner, just click on that.
c. Then after it will pop-up an APT Url just type their cydia[17] website and click on add source.
d. After that, it will again pop up an dialogue box which will ask for permission either add anyway or cancel, just click on add anyway.
e. Now it will accepted by iPhone and added into your sources, just click over that.
f. After that go for I section which includes installous[18], just click install that too, because it will give the intermediate path to install the third party packaged software run by cydia.

Now onwards, go to the search box and search for downloads. Here, new software we need to have install, that is called Hian Zin Jong that is download manager (like internet download manager in windows). This really helps to successful implementation of this proposed system because it makes the faster download for iPhone; perhaps, it is also third party software package but did a great effort to complete this analysis. After download this Hian Zin Jong software[7], we are moving to download main Counter strike game which is portable by Unity 3d Game Engine. Now let's have some serious moves toward this proposed system.

Fig 4-Hian Zin Jong a Download manager

5. COUNTER SRTIKE BY UNITY GAME ENGINE

Unity is an integrated authoring tool for creating 3D video games or other interactive content such as architectural visualizations or real-time 3D animations. Unity's development environment runs on Microsoft Windows and Mac OS X, and the games it produces can be run on Windows, Mac, Xbox 360, PlayStation 3, Wii, iPad, iPhone, as well as the Android platform. It can also produce browser games that use the Unity web player plug-in, supported on Mac and Windows and coming to Linux. The web player is also used for deployment as Mac widgets. Unity also has the ability to export games to Adobe's Stage 3D functionality in Flash, but certain features that the web player supports are not usable due to limitations in Flash. Counter strike game is become fully portable by the help of Unity 3d game. Unity game is basically written in either C++ or C# to develop any game. So it is much easier to understand and will run it with less requirement of processor and other equipment. This time counter-strike game is also portablised by Unity games.

To access the software package of Counter-Strike and make it compatibly accesses just go to the Counter-Strike Portable Site [6]. This will easily gives a web page of Counter-Strike, means a web portal for Counter –Strike. After doing this just follow these steps to access the software for your iPhone.

a. Click on downloads tab at the top of the web page, it will shows two option iOS or Android chose any one according to your need or say your phone.
   b. I choose iOS because this paper is inclined to iOS so, it will pop-up a new window which shows CS Portable 1.97c [iOS], Just download it.
   c. It will show some time to start downloading, so let it be.
   d. After downloading, it will show a file named CSportable.ipa
   e. Now, make it in working form you should have to redirect this downloaded file into installous which is an application of Cydia.
   f. So here either chose iTunes from your computer to change the file location of this ipa file or you should download iFile, which is also available at Cydia.
   g. Here, this process is done by iFile, third party software, by which I recommended to mark and move the file location from mobile downloads to installed application then downloads, so this whole process will be done by like this, go to mobile downloads then click edit option, after that new window pop-up click upon copy/link then move to installous and paste it over here.
   h. Now click on that and then a new windows will pop-up, we have to select install to run this ipa file and that's all the process will be run by iPhone.

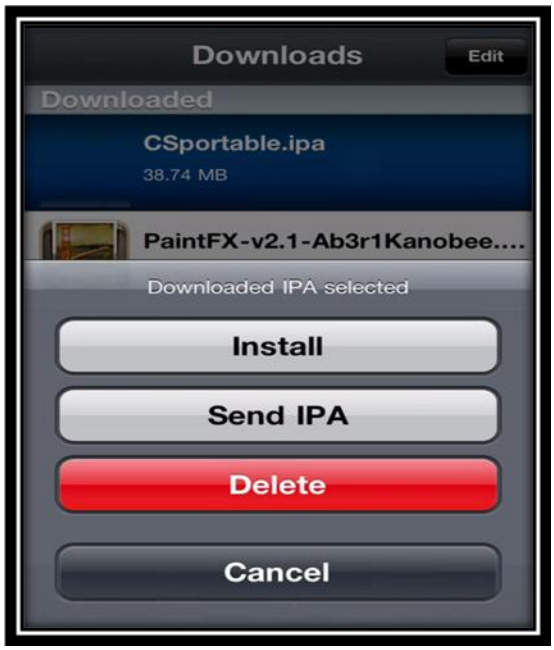

Fig 5- Installation of CSportable IPA

i. In android, there is no need to do all that kind of stuff because it is not necessary in case of android because, it is developed upon java and we already

know that java is platform independent language so you have to simply go to the web site of Counter-Strike[5] and just download the apk file and run it.

j. Now, after installing the ipa file in iPhone, just run it.

After successfully doing all these things unity portable Counter-Strike game will work in successful manner.

6. CONCLUSION

Conclusively, in the below, all figures shows the fully functioned game, Counter-Strike in iPhone and in Android too, the first figure, Fig 6 demonstrating the initial booting of the game which runs the code to access the cs-portable game. Fig 7 demonstrating the play mode of game fully functioned and last one in which I demonstrate the controlling instructions.

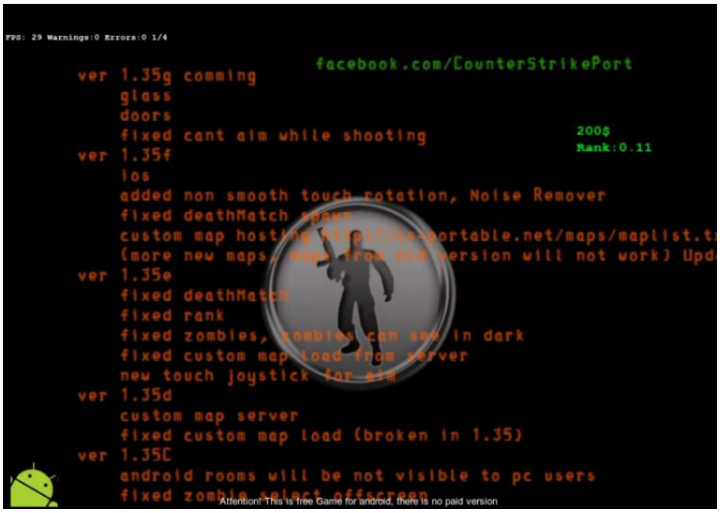

Fig 6- Boot time in android

Fig 7- Play mode in iPhone

This shows that device is now ready to play the game on your iPhone or Android device. It only happens when your device will fulfill the requirement of the software to make it run. The main issue arises to run this software package into iPhone, is the software certificate which is not authorize by apple privacy threats, but here we just assign the authentication, which easily bypass the privacy agreement and yes the jailbreak is legal[19], so don't panic this will up to user either he/she will want it or not. Conclusively, it will maintained your game freakiness without any harm of your iPhone and more appropriately it will also gives a platform to make your iPhone compatible to Game.

Fig 8- Instruction in iPhone

7. REFERENCE

[1]How to Install Non-Market Apps on Your Android Device,http://www.howtogeek.com/howto/41082/install-non-market-apps-on-your-android-device/

[2] Downloads for iPad - Download Manager http://itunes.apple.com/in/app/downloads-for-ipad-download/id380641055?mt=8

[3] Gartner Newsroom. Competitive Landscape: Mobile Devices, Worldwide, 2Q10. http://www.gartner.com/it/page.jsp?id=1421013

[4] Counter Strike Unofficially Ported To Android Devices [Download]http://phandroid.com/2012/01/21/counter-strike-unofficially-ported-to-android-devices-download/

[5] Pod2G: iOS 5 Untethered Jailbreak Code Complete For All A4 Devices http://www.theiphonespot.net/pod2g-ios-5-untethered-jailbreak-code-complete-for-all-a4-devices/

[6] Expert iPhone Jailbreaking Instructionshttp://iphonejailbreaknews.com/

[7] This Is How You can Help Pod2G Jailbreak The iOS 5.1 Firmware Untethered http://www.ijailbreak.com/jailbreak/help-pod2g-jailbreak-ios-5-1-untethered/

[8] Download and Play Counter Strike (CS) FPS Game On Android http://www.pressbyte.com/8121/download-play-counter-strike-cs-fps-game-android/
[9]CounterStrikeSource
http://store.steampowered.com/css
[10] OTRS iPhone App Demo Configuration http://www.otrs.com/fileadmin/mediafiles/Produkt/OTRS_iPhone_App/Demo_files/OTRS_iPhone_Demo_Conf-ENG.pdf
[11] Counter Strike the Untold Story of America's Secret Campaign against Al-Qaeda, http://osgoodcenter.org/CounterStrikeCR.pdf
[12]Android Market, http://www.android.com/market.
[13] Secure your Jailbroken iPhone from SSH Hacking With MobileTerminal App http://jaxov.com/2009/11/secure-your-jailbroked-iphone-from-ssh-hacking-with-mobileterminal-app/
[14] Welcome to Hex-Rays!http://www.hex-rays.com/
[15] Jailbroken stats: Recent survey suggests 8.43% of iPhone users jailbreak http://www.iphonefreak.com/2009/08/jailbroken-stats-recent-survey-suggests-843-of-iphone-users-jailbreak.html
[16]
http://www.smi.ethz.ch/education/courses/UserInnovation/studentpresentationsUI/UI_HS2011_CounterStrike.pdf
[17]This is Hackulo.us's official Cydia repository.http://cydia.hackulo.us/
[18] Download installous http://cydia.hackulo.us/installous-5.0-9.deb
[19] Statement of the Librarian of Congress Relating to Section 1201 Rulemaking http://www.copyright.gov/1201/2010/Librarian-of-Congress-1201-Statement.html
[20]hitbsecconf2012ams
http://conference.hitb.org/hitbsecconf2012ams/ios-jailbreak-dream-team-releases-absinthe-2-0-ios-5-1-1-jailbreak/
[21]iPhone Research Paper http://mad-ip.eu/files/reports/iPhone.pdf
[22] iOS 4.2.1 Jailbreak https://www.it-security-experts.co.uk/component/content/article/308.pdf
[23] Ethical Implications of Modifying Modern Mobile Computing Platforms http://www.justonwestern.com/auburn/MobileComputingEthics.pdf
[24]iPhone Developer Program License Agreement
http://www.seclab.tuwien.ac.at/papers/egele-ndss11.pdf
[25]A. Cohen. The iPhone Jailbreak: A Win Against Copyright Creep. http://www.time.com/time/nation/article/0,8599,2006956,00.html.
[26]N. Seriot. iPhone Privacy. http://www.blackhat.com/presentations/bh-dc-10/Seriot_Nicolas/BlackHat-DC-2010-Seriot-iPhone%2dPrivacy-slides.pdf.
[27] Save your SHSH blobs for iOS 5.1.1 http://www.idownloadblog.com/2012/05/25/save-your-shsh-blobs-5-1-1/
[28]APTicket
http://theiphonewiki.com/wiki/index.php?title=APTicket
[29]ECID
http://theiphonewiki.com/wiki/index.php?title=ECID
[30]SHSH Protocol
http://theiphonewiki.com/wiki/index.php?title=SHSH_Protocol
[31] Counter-Strike Game application http://cs-portable.com
[32] Absinthe 2.0 has arrived! http://greenpois0n.com