Hacking iPod Touch/iPhone

Marcos Azevedo

(psylinux)

Apresentação

Marcos A.T. Azevedo:

- Cientista da Computação e Aluno de Mestrado em Sistemas Distribuidos pela Universidade Federal e Goiás.
- Iniciou sua jornada pelo mundo do softwarelivre em 1993.
- É um dos Fundadores do PSL/GO (Projeto Software Livre de Goiás) e da ASL/GO (Associação de Software Livre de Goiás).
- Atualmente tem se ocupado no desenvolvimento deaplicações para RSSF (Redes de Sensores sem Fio) e em um sensor de medição de Fluxo baseado em ultra-som.
- Como grande entusiasta do Software Livre, tem Palestrado sobre vários Tópicos relacionados a Linux e Software Livre em eventos como: FGSL, FISOL, Jornada Tecnológica do Senac, Semana Tecnológica da Universo etc.
- Principais interesses são:RSSF e Sistemas Distribuidos, Robótica, Inteligência Artificial, Protocolos de Comunicação, Segurançae Kernel Hacking.

The Ipod Touch

Resources

- Processor: 400MHz Arm
- RAM: 128Mb
- Storage: 16 Gb
- Screen: 3.5”
- Weight: 120 g
- OS: OS X (Darwin)
- Wireless: 802.11b/g
- Cost: U$ 400

Tiff Exploit

- Developed by Niacin and Dre
- On your iPod touch, navigate in Safari to
  - ✓ http://jailbreak.toc2rta.com
- It will crash your Safari and return you to the homescreen, but this is expected

Tiff Exploit

Let’s take a look at the Code

Tiff Exploit

```
% g++ itiff_exploit.cpp
% ./a.out 1.1.1 > crack.tiff
% cp crack.tiff~/public_html
% sudo /etc/init.d/apache2 start
```

Jailbreak iPod

- The iPHUC
- Brought jailbreak, iActivator, newgshell, ipiinto a package that is maintainable and opensource under the GPL.
- Download http://code.google.com/p/iphuc/

iPHUC

- Type ./iphuc and hit return

- Type the following into the iPHUC terminal:

```
getfile /dev/rdisk0s1 iphonefs/rdisk0s1 314572800
```

- Once complete, there will be a file named "rdisk0s1" in your "iphonefs" folder

iPHUC

- Add .dmg to the end of the file. It should end up being rdisk0s1.dmg
- Double click the file to mount it
- Modify the fstab for the new System
- Back in iPHUC Terminal:

```
putfile iphonefs/rdisk0s1.dmg /dev/rdisk0s1
```

- When it's finished, reboot the iPod Touch

Installing SSH

- Download iNdependence from its Google code page:

  http://independence.googlecode.com/files/iNdependence_v1.2.1a_bin.dmg

  - Click "Install SSH/SFTP/SCP" and follow the instructions. It will ask to reboot the iPod Touch several tim

Installing SSH

- When you're done, reboot your iPod Touch one more time, then SSH into your iPod Touch from the Terminal by typing the following:

```
ssh -l root your.ipods.ip.address
```

Protocols: SFTP/SSH

server: your iPod's local ip address

user: root

password: alpine

Fix iTunes Syncing

- Logged in SSH, navigate to /var/root and rename Media to Media_sym
- Rename Mediaold to Media. Keep the FTP and SSH windows open.
- Open iTunes and allow it to activate. If it doesn't recognize your iPod, reboot it and/or restart iTunes.

Tips and Tricks

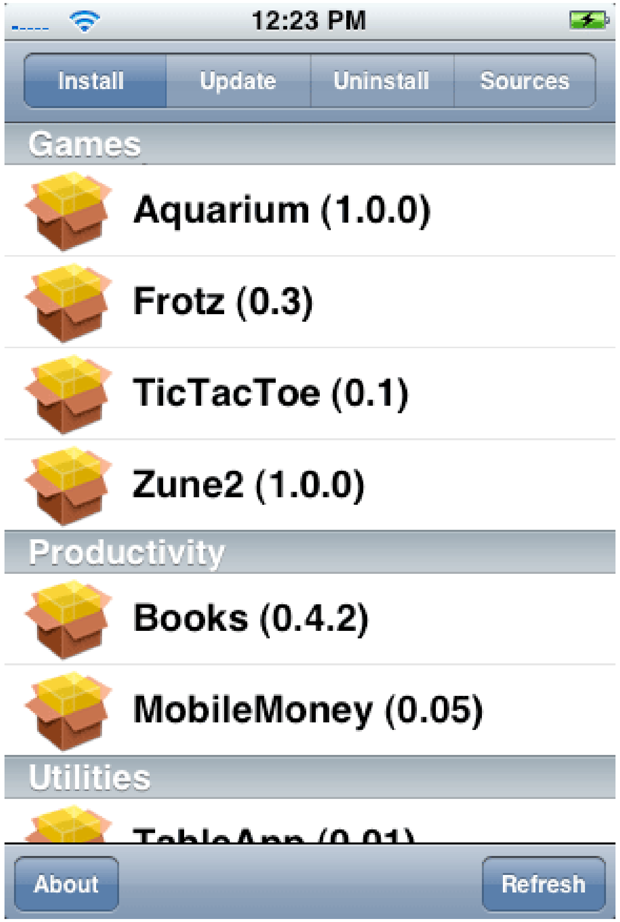
- /dev/rdisk0s1= 300 Mb
  - ✓Space for Firmware and Apps
- /dev/rdisk0s2 = 16 Gb
  - ✓Space for Media (Audio/Video)
- Create symbolic link for:
  - /opt
  - /Applications

Demonstration

Time for Demo

Install Installer.app

- Download Nullriver's Installer.app from http://iphone.nullriver.com/



Games

Aquarium (1.0.0)

Frotz (0.3)

TicTacToe (0.1)

Zune2 (1.0.0)

Productivity

Books (0.4.2)

MobileMoney (0.05)

Utilities

TableApp (0.01)

Install Apache/Lighttp

- Use the Tapp (Installer.app)
- Just a couple clicks

iJailBreak

- Download it from:

  http://www.ijailbreak.com/

1. Run the software
2. Follow the steps
3. Enjoy your hacked iPod/iPhone

Thanks and Questions

E-mail: marcos@psylinux.org