pod2g's iOS blog

Apple iOS Security Research [*note that I'm against piracy: no sim unlock, installous, xsellize, etc.*]

FRIDAY, FEBRUARY 24, 2012

A working GNU Debugger on iOS >= 4.3

People know that the gdb package coming from Cydia is broken since 4.3.

But here is a simple way to have a working gdb running on your iOS device : use the one from the Apple SDK !

Prerequisites :
- a jailbroken iOS >= 4.3 device
- OpenSSH should be installed on the iOS device and should listen for connections
- an OSX machine with the iOS SDK >= 4.3 installed

How to :
- remove the gdb package from Cydia
- do the following in the OSX terminal :

```
cd /tmp
cp /Developer/Platforms/iPhoneOS.platform/Developer/usr/libexec/gdb/gdb-arm-apple-darwin .
lipo -thin armv7 gdb-arm-apple-darwin -output gdb
nano entitlements.xml
```

- paste the following to the OSX terminal :

```
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>com.apple.springboard.debugapplications</key>
        <true/>
        <key>get-task-allow</key>
        <true/>
        <key>task_for_pid-allow</key>
        <true/>
</dict>
</plist>
```

- save the file by doing CTRL + X, then 'Y', then 'ENTER'

- now do the following in the OSX terminal :

```
ldid -Sentitlements.xml gdb
scp gdb root@<iOS Device IP Address>:/usr/bin/
```

- GDB is now installed to your iOS device.

Happy debugging !

~pod2g

Publié par pod2g à l'adresse 12:04 AM

Newer Post Home Older Post