A Close-Up on Jailbreaking and Tweak Development

Nikias Bassen

@pimskeks
nikias@samara-it.de

September 29, 2012

Outline

- About Me
- Jailbreaking
- Tweak Development

About Me (1)

- IT expert from Germany, CEO @ samaraIT
- Involved in RE and Security for almost 15 years
- Studied Computer Science in Bremen, Germany
- Linux Developer (yes, I don’t have a Mac!)
- First iPhone 2008
- Joined usbmuxd & libimobiledevice projects

About Me (2)

- RE of iTunes/iPhone communication protocols to make usbmuxd & libimobiledevice possible
- RE of iTunes database hashing algorithm to bring Linux music sync support
- iOS RE and Security Research
- Tweak development since 2010
- Joined Chronic-Dev in 2011 and worked on Absinthe & Absinthe 2.0 Jailbreaks

Jailbreaking

Jailbreaking (1)

- Why work on a jailbreak?
  - ➡ It's fun!
  - ➡ Really challenging field for security research due to the numerous iOS security features
- How to create a jailbreak?
  - ➡ Injection vector, root filesystem access, codesign exploit, sandbox escape, kernel exploit, ASLR …

Jailbreaking (2)

- My involvement in Absinthe & Absinthe 2.0
  - ➡ Libimobiledevice device handling code
  - ➡ MobileBackup2 payload injection
  - ➡ MobileBackup crash & crash report evaluation
  - ➡ Directory traversal using AFC & MobileBackup2

Jailbreaking (3)

- 'Is it dangerous?'
  - No! Jailbreaks are usually just local exploits.
  - But change passwords if you install OpenSSH!
- 'I am afraid of jailbreaking my device!'
  - Don't be! It's a software modification and completely reversible by a firmware restore

Jailbreaking (4)

- Why should I jailbreak my device?
- It's your device, you should be allowed to do whatever you want with it
- The JB community provides thousands of tweaks, themes, and apps that improve device usability, the 'look and feel' or add new features

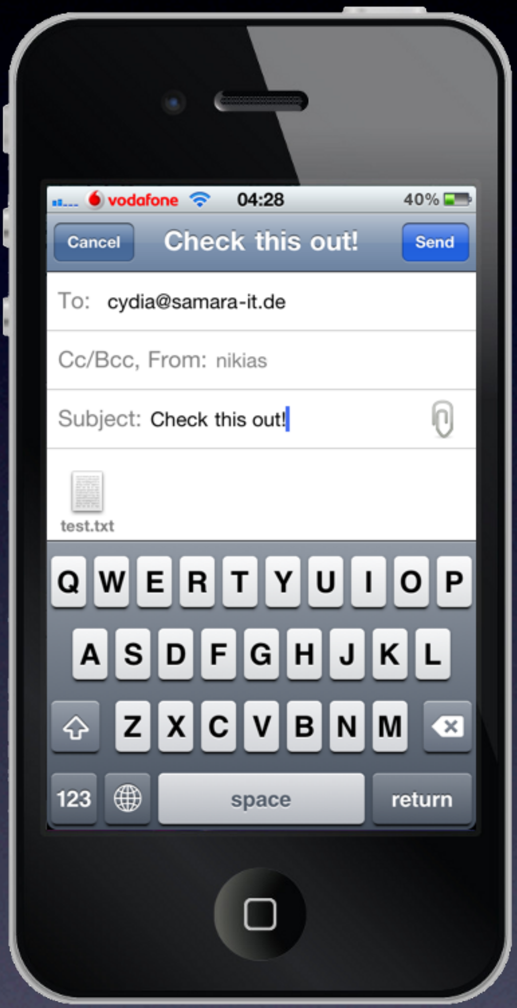
This is just awesome!

Tweak Development

Tweak Development

- What is a tweak and how do they work?
  - ➡ Extending or changing the behavior of an app
  - ➡ Achieved by hooking Objective-C or C/C++ methods/functions and adding custom code, usually using MobileSubstrate

Tweak Development



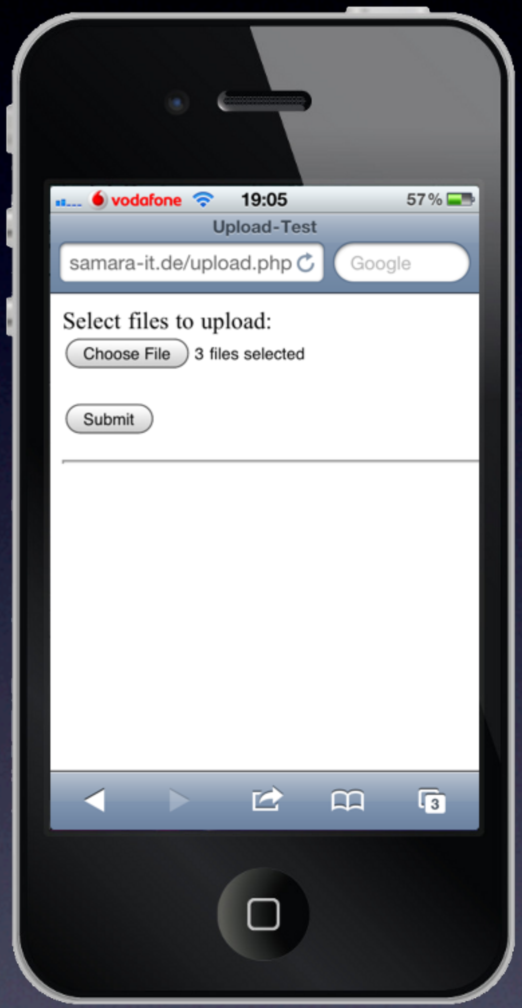
To: cydia@samara-it.de

Cc/Bcc, From: nikias

Subject: Check this out!

test.txt

AnyAttach



Upload-Test

samara-it.de/upload.php

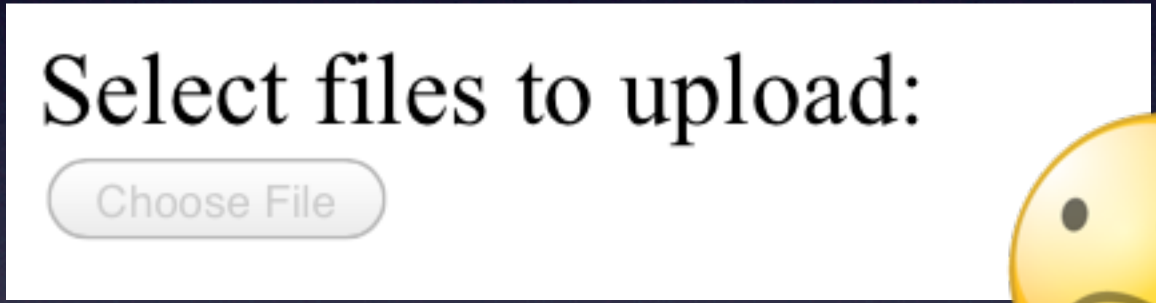
Select files to upload:

3 files selected

Safari Upload Enabler

Tweak Development Example: Safari Upload Enabler

- How did the idea come up?
- Random webmail page:



Select files to upload:

- So, just enable that button?!

Tweak Development Example (2): Safari Upload Enabler

- It's not only about MobileSafari, but WebCore
- WebCore is written in C++, not ObjC
- So: MobileSubstrate C++ function hooking!
- MobileSafari needs a file picker (ObjC)

Tweak Development Example (3): Safari Upload Enabler

- Tweaking WebCore
  - ➡ File upload code already present since iOS 4
  - ➡ Problem 1: Enable the Button
  - ➡ Problem 2: Add files for uploading
- Tweaking MobileSafari
  - ➡ Add a file picker!

Tweak Development Example (4): Safari Upload Enabler

- WebCore Problem 1: Enable the button
  - ➡ Disabled right after creation and when changing the type of an HTML <input> tag to 'file'
  - ➡ Hook and change setDisabled() function
  - ➡ Hook creation of <input> elements and re-enable if it's of type 'file' using the above hook
  - ➡ Hook function setting the input type and re-enable it as well

Tweak Development Example (5): Safari Upload Enabler

- WebCore Problem 2: Add files for uploading
  - ➡ The <input> element has a file list, but adding a file requires a bunch of hooks
  - ➡ Create a 'File' object
  - ➡ Expand the file list
  - ➡ Append the file to the list
  - ➡ Notify <input> element has been updated

Tweak Development Example (6): Safari Upload Enabler

- Still sounds easier than it is!
    - ➡ Accessing C++ member variables by offset
    - ➡ New offsets if WebCore is updated
    - ➡ Required to use internal String and Malloc functions to make it NOT crash Safari
    - ➡ Moreover, the file upload control should also visually reflect the file selection: '3 files selected'
    - ➡ Total of 52 C++ function hooks

Tweak Development Example (7): Safari Upload Enabler

- MobileSafari: Adding a file picker
  - Create UIKit file selection dialog
  - But MobileSafari is sandboxed, so file access is very limited
  - Working around this by using westbaer's sandcastle tweak
  - Additional functionality: Photo/Video picker, Dropbox integration

Tweak Development Example (8): Safari Upload Enabler

- iOS 6 now allows native photo/video uploading
- Update is already worked on to bring full upload capabilities back!

Questions?

@pimskeks

nikias@samara-it.de