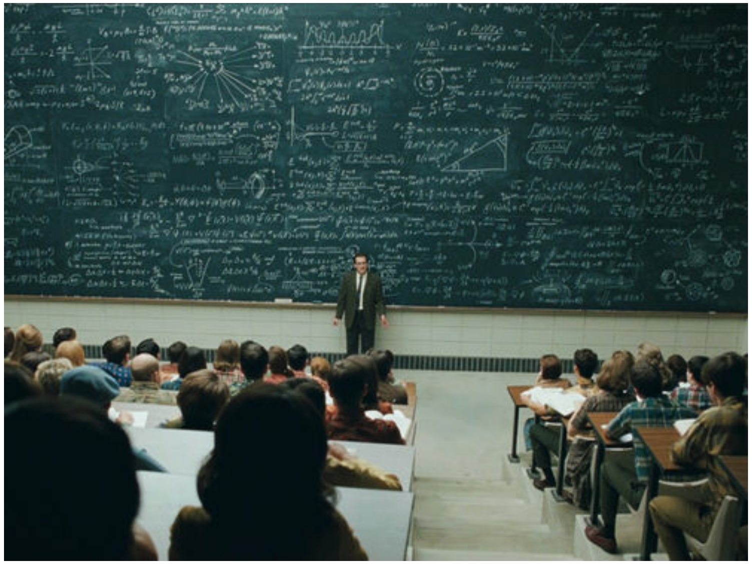
Mobile Hacking VI

iOS Jailbreak

Crakun
Tues, 10-1-13 2nd day of class

Mobile Hacking VI
Class Agenda

- Part I:
  - Intro /Building a Team
  - Jailbreak Development Roadmap
  - Questions
- Part II
  - Jailbreak History
  - Fuzzing and .mov files
  - Homework Assignment
  - Open Floor



Part I

- Intro /Building a Team
- Jailbreak Development Roadmap
- Questions

About Me

Crakun’s Metadata Graph:

Age:	19
Born:	Nov 31, 1995
Place of Birth:	Korriban
Hobbies:	Badminton, Karaoke, Mobile
Favorite Food:	Moo Goo Gai Pan
Occupation:	Part-time Scuba Diver
Role Model:	Riddick

Crackun Contact Info

Email: crakun@m0bdev.com
Twitter: crakun
Skype: m0bdev
IRC: #openjailbreak on freenode

(m0bdev is spelled with a zero)

HOtWAN

Goal

The Goal of this class is to build an iOS untethered Jailbreak from scratch by creating a new Community-based Jailbreak Team

Mobile Hacking VI
Class Schedule

- Weekly Class is migrating to Saturdays, 6am PST
- Next meeting (day 3): Sat, Oct 5, 2013 6am PST

Mobile Hacking VI
Class Topics

- Jailbreak Project Status / Questions

- Focal Points of Discussion
  - ARM, Crash Dumps, Kernel Panics, KASLR, etc.
  - Reverse Engineering and Exploit Techniques

- From time to time, maybe Special Guests / Commentary

Mobile Hacking VI
Expectations / Assumptions

- I am not charging you money for this version of the Class.
- I have a part-time day job in Hawaii. Hence, I am not in a rush to race thru this class' Jailbreak
- This is not a spoon-fed class. There is a lot of hard work to be done on your part
- Active participation is required on your part.

- This is a hands on class that requires a contributing community in order for it to Succeed
- Code developed for Open Community Group is opensourced with a BSD license

Building a Jailbreak Team

- m0bdev
  - Open Community Group
  - Core Group

- Roles
  - Administrative Assistance
  - Info Researchers
  - Architecture Design for JB
  - Bug Finding
  - Vulnerability Analysis / Reverse Engineering
  - Exploitation Development
  - Implementation /Distribution

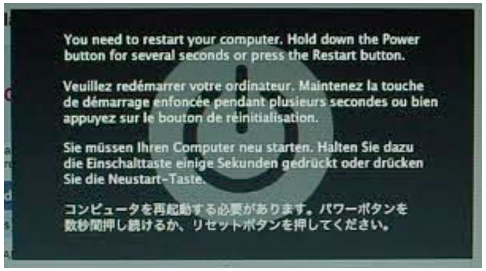
m0bdev
Jailbreak Expectations / Assumptions

- m0bdev Team (spelled with a zero)
  - Open Community Group is for everyone/ anyone to join
  - Core Group
- Apple is most likely listening.

- We start fresh in terms discovering Vulns
  - Bugs/ Vulns / Exploits donated in class will be burned in the Jailbreak Process.
  - This is a class effort.
  - Credit will be noted when/ if possible.
  - Due to the Openess of this development, some people / companies / countries will try and take your credit. Perhaps develop a full jailbreak on their own before we finish as a class
- This jailbreak exercise will take lots and lots of time.
  - This is a learning process for all. Very steep learning curve for most.
  - We are not racing / competiting
  - Jailbreak process / approach may likely change overtime

Bugs, Vulns, Exploits we are looking for in class

- Remote Exploits
- Userland Vulnerabilities(to obtain mobile)
- Privilege escalation (mobile to root)
- Escaping sandbox techniques
- Memory leaks
- Bypassing code signing techniques
- Kernel Vulnerabilities
- Strategies for dealing with KASLR on 64-bit ARM



You need to restart your computer. Hold down the Power button for several seconds or press the Restart button.

Veuillez redémarrer votre ordinateur. Maintenez la touche de démarrage enfoncée pendant plusieurs secondes ou bien appuyez sur le bouton de réinitialisation.

Sie müssen Ihren Computer neu starten. Halten Sie dazu die Einschalttaste einige Sekunden gedrückt oder drücken Sie die Neustart-Taste.

コンピュータを再起動する必要があります。パワーボタンを数秒間押し続けるか、リセットボタンを押してください。

Jailbreak Development Roadmap
1st Steps

- Identify Volunteers. (folks from class)

- Send me an email:
  - which role(s) you want to help out in.
  - Your skills sets
    - What you are good at
    - Seek to improve on
    - Be realistic

- Review Jailbreak Exploit History

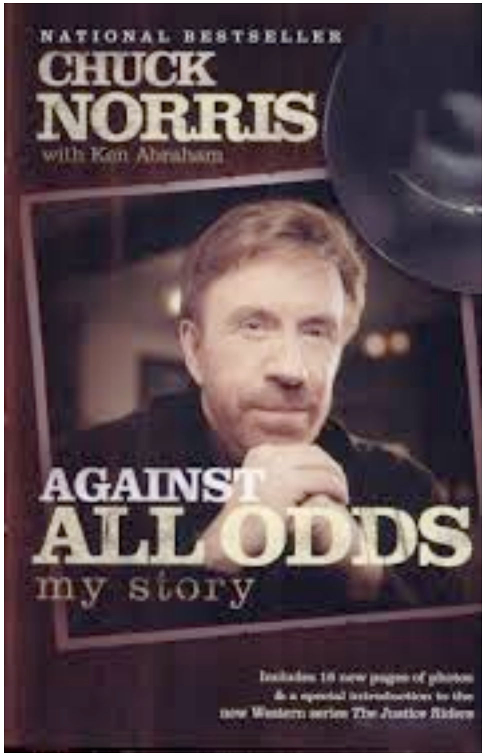
- Start working on a remote userland exploit

- Set up Repositories for Documentation, Tools, Code development (We are in process of doing that)

m0bdev’s
Jailbreak Development Targets

- For Open Community Group, we will be openly developing an untethered jailbreak for:
  - iPhone 4 (7.0.2)
  - iPhone 5 (7.0.2)
- For Core Group, we will be developing an untethered jailbreak for:
  - iPhone 5S (7.0.2)
- We are standardizing on iPhone4 (6.1.2) where you have your SHSH Blobs already saved for (6.1.2) and (7.0.2)
- You can use your already other Jailbroken devices to help find bugs, vulns and develop exploits for the class.

Questions ?


NATIONAL BESTSELLER
CHUCK NORRIS
with Ken Abraham
AGAINST ALL ODDS
my story
Includes 16 new pages of photos & a special introduction to the new Western series The Justice Riders

- IRC
- Skype
- Email
- I may not have all the answers instantly, but may need to follow-up later if it makes sense and I have time.
- I may get things wrong, but feel free to correct me.

HOtWAN

Part II

- Jailbreak History
- Fuzzing and .mov Files
- Homework Assignment
- Open Floor

Jailbreak Exploit History

- Previous Jailbreak History
  - Essential for Architecture Design for JB
  - Implementation /Distribution
- http://www.trailofbits.com/resources/ios_jailbreak_analysis_slides.pdf
- http://conference.hitb.org/hitbsecconf2013ams/materials/D2T1%20-%20Pod2g,%20Planetbeing,%20Musclenerd%20and%20Pimskeks%20aka%20Evad3rs%20-%20Swiping%20Through%20Modern%20Security%20Features.pdf
- http://theiphonewiki.com

Fuzzing .mov Files
POP QUIZ

- What is the service that is provides for playing .mov files on the iPhone 4 /5 / 5S?

- Name some Existing Fuzzers that target files that we could use for .mov files?

- Have there been any documented vulnerabilities with .mov files?

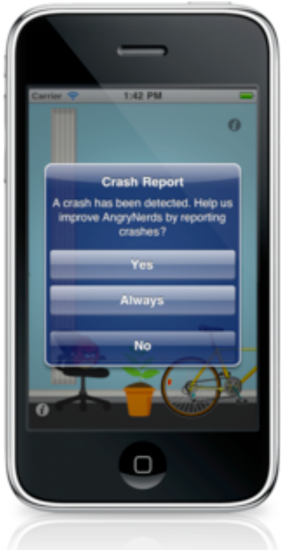
- Explain to me about the file format of .mov files?

- How might we test fuzzed .mov files?

- How can we automate the process for testing?

Fuzzing .mov Files

- Any crashes so far? (don't send them to Apple)
- Do we need to build a custom .mov file fuzzer?
  - http://shakacon.org/2009/talks/Exploit_or_Exception__DeMott.pdf
  - http://www.blackhat.com/presentations/bh-usa-05/bh-us-05-sutton.pdf
  - http://www.cert.org/vuls/discovery/bff.html
  - http://peachfuzzer.com/v3/TutorialFileFuzzing.html
  - Chapter 6: iOS Hacker's Handbook
  - https://developer.apple.com/standards/classicquicktime.html



Crash Report

A crash has been detected. Help us improve AngryNerds by reporting crashes?

HOtWAN

Homework Assignment

- Review slide deck.
  - Think about what you can do. Let me know.
  - Contact me if you want to share bugs, confirmed vulns, exploits via Email or Skype
  - Come up with thoughtful suggestions for class format.
  - Send me questions you have that pertain to the class Jailbreak

- Continue on:
  - Fuzzing .mov files and answer POP quiz questions
  - Send me info for m0bdev Open Community Distribution:
    - Find file fuzzing tools where the source code is available
    - .mov file format
    - Be the first to find an exploitable remote vuln so the class as a whole can move forward

- Spread the Word

Open Floor Discussion

- We are listening

Extra

Sk00l Supplies
Software / Hardware

- Xcode (run latest version)
- IDA Pro
- Gdb
- OxED   http://www.suavetech.com/0xed/
- Mac book running Mountain Lion
- Serial Debugging Cable
- WiFi
- Jailbroken iPhone4/5 (6.1.2)
- UnJailbroken iPhone4 (7.0.2)
- UnJailbroken 5/5S (7.0.2)

Great Starter Books

- Mac OSX and iOS Internals
- Hacking and Securing iOS Applications
- iOS Hacker’s Handbook
- Mac Hacker’s Handbook
- OSX and iOS Kernel Programming
- Cocoa Application Security
- C in a nutshell
- ARM Assembly Language Fundamentals & Techniques
- ARM Assembly Language –An Introduction