Mobile Hacking VI

m0bdev

iOS Jailbreak

Crakun

mo -metadata: http://www.youtube.com/watch?v=9HGMxZEl60k

Sat, 11-23-13, 6am PST Day 10

Mobile Hacking VI
Class Agenda

- Part I:
  - Communications
  - KASLR, Panic Logs, Link State Analysis

- Part II
  - Homework

m0bdev Jailbreak Team

Jailbreak Codename:

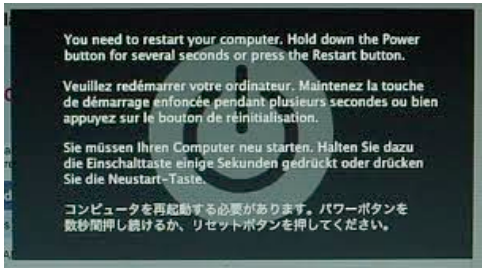
chemrail

An Analogy,…

http://www.youtube.com/watch?v=oIBtePb-dGY

Bugs, Vulns, Exploits we are looking for in class

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



Communications

crakun contact Info

Email: crakun@m0bdev.com

Twitter: @crakun

Skype: m0bdev (m0bdev is spelled with a zero)

IRC: #openjailbreak on freenode

**-> If I am slow responding / or no response, ping me again because I may have missed it

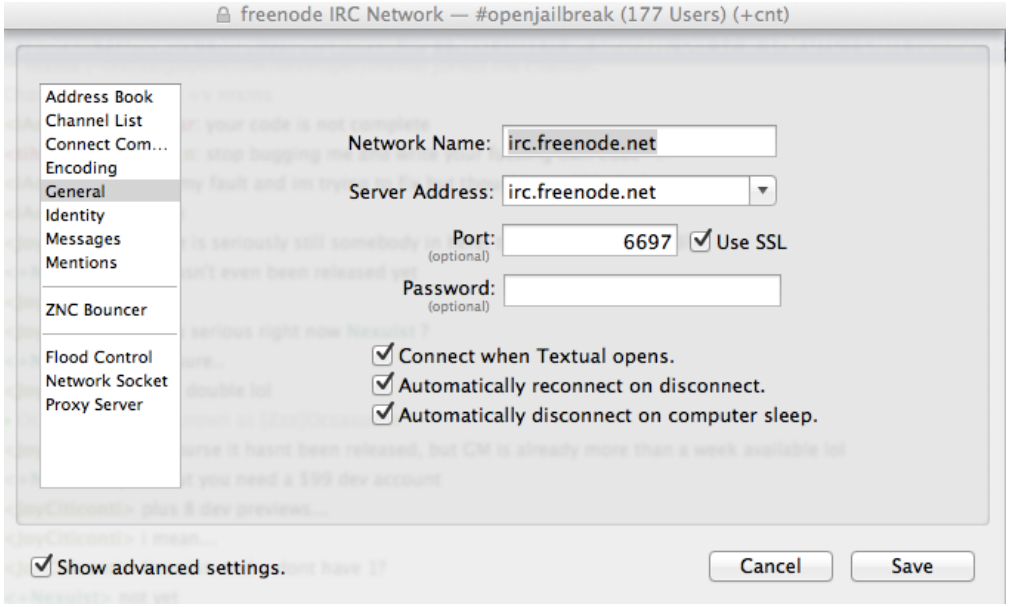
Submittal for Bugs/ Vulns /Exploits

Email Me (crakun@m0bdev.com) with a zip file of:

1. Detail Step-by-Step Method how / what you did so I can reproduce it
2. What devices and firmware does this occur on?
3. Tell me what you think it is?
4. Include Crash Report / Panic Log
5. Include Proof-of-Concept source code
6. Put a date on the submission

Class Communications

Text -> IRC: #openjailbreak on freenode



Skype: m0bdev (m0bdev is spelled with a zero)

Please mute Skype unless you have a question during clazz

KASLR

Randomizes the physical and virtual address at which the kernel image is decompressed

As a security feature that deters exploit attempts relying on knowledge of the location of kernel internals.

Kernel Panic

Panic Log Analysis

Verify the crash dump in Settings / General / About / Diagnostics & Usage / Diagnostic & Usage Data is enabled.

/var/mobile/Library/Logs/CrashReporter/Panics/ for kernel panics

Kernel Panic logs are stored in /private/var/mobile/Library/Logs/panic.log if there is no panic.log file you have to create one***

Link State Analysis

Data link analysis is a technique used to evaluate relationships (connections) between nodes. Relationships may be identified among various types of nodes (objects).

Data points within Panic logs will be used to derive an algorithm in hopes to defeating KASLR.

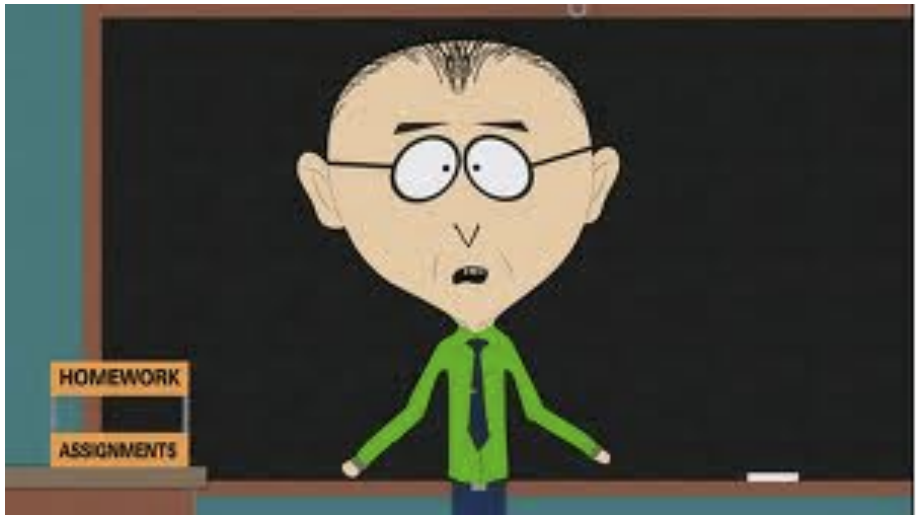
This is another approach instead of using information leaks.

Link State Analysis Analogy

The Big Bang = boot

Constellation = kernel memory

Homework



Homework Assignment

1. Power off your device such that a passcode is not required.
2. Power on your device.
3. Open up Safari and navigate to www.hotwan.com/a.mov
4. Device should reboot, pull panic log off assign it a number.
5. Power off your device.
6. Repeat steps 2-5 for 100 times

7. Email the panic logs in a zip file along with a text file of the model number, type of device and firmware version to: crakun@m0bdev.com. For the Subject line use: KASLR Link State Analysis

Homework Assignment

- Review slide deck.
  - Think about what you can do.

  - Contact me if you want to share bugs, confirmed vulns, exploits via Email: crakun@m0bdev.com

- New Comers: (review previous slides decks from hotwan.com/class/ and reddit for logs. Audio is out there too on the Internet

Next Meeting:
(Day 11): Sat, Nov 30, 2013 6am PST

- Fuzzing Safari and Javascript.

Open Floor Discussion