EXHIBIT I

DECLARATION OF RYAN BRICKER IN SUPPORT OF *EX PARTE* MOTION FOR TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INUNCTION; ORDER OF IMPOUNDMENT

HackMii

Notes from inside your Wii

- front page
- archives
- about
- RSS

```
1C 28  ADDS    R0, R5, #0                ; R0 = R5
38 14  SUBS    R0, #20                   ; R0 -= 20
99 02  LDR     R1, [SP,#0xA44+SHA1_in]   ; R1 = SHA1_in
22 14  MOVS    R2, #20                   ; R2 = 20
4B 0F  LDR     R3, =(strncmp+1)          ;
47 98  BLX     R3                        ; strncmp(cert[cert_size - 20], SHA1_in, 20)
28 00  CMP     R0, #0                    ;
```


Categories

- dsi
- Other consoles
- Wii

Archives

- December 2010
- November 2010
- September 2010
- August 2010
- July 2010
- June 2010
- May 2010
- April 2010
- February 2010
- January 2010
- December 2009
- November 2009
- October 2009
- September 2009
- August 2009
- July 2009
- June 2009
- May 2009
- April 2009
- March 2009
- February 2009
- January 2009
- December 2008
- November 2008
- October 2008
- September 2008
- August 2008
- July 2008
- June 2008
- May 2008
- April 2008

Admin

- Register
- Log in

← Dear Nintendo, Even More NAND Flash Hax →

xyzzy

July 22nd, 2008 by bushing · 43 Comments

This isn't the prettiest code I've ever written — it doesn't have much of an interface, and I just threw this release together in a few minutes. However, it's been exceedingly useful to me, and hopefully some of you will find it useful, too. I'll quote the README here:

This program will do the following, automatically:

- Download IOS11 from the Nintendo Update Server
- Patch it to remove the MEM2 protection (so the PPC can access all 64MB of it)
- Patch it to allow it to delete itself later using ES_DeleteTitle()
- Find an unused IOS slot (counting downward from IOS255)
- Install the hacked IOS11 there
- Reboot into the hacked IOS
- Copy the private key structure from the IOS address space into MEM1
- Reboot back into a sane IOS
- Delete the temporary, hacked IOS
- Display the keys on screen
- Try to write them to a file on the SD card — keys.txt
- Pause for 60 seconds to allow you to copy the keys down using pen and paper,if necessary

I wrote this a week or two after I killed a Wii trying to reproduce tmbinc's original Tweezer Hack. May it rest in peace.

The first version of this code just used a patched version of IOS, which was an ugly hack. It's still an ugly hack, but at least it no longer contains copyrighted code. You should only really need to run it once on any given Wii, but it should be safe to run as much as you want. If nothing else, it demonstrates the kinds of ways you can use PatchMii_core to do something useful (as opposed to just running it and then packaging the result up as cIOS).

(c) 2008 bushing / hackmii.com

Download: xyzzy-1.0.zip (source and binary)

Tags: Wii

43 responses so far ↓

- 1 **bushing** // Jul 22, 2008 at 6:17 pm

  If anyone asks me what the point of this program is or why they need these keys or how to use them, I'm going to hit them.

- 2 **Stalkid64** // Jul 22, 2008 at 6:25 pm

  Damn that was my first questions. :*(
  <3 xyzzy.dol

- 3 **ProdigySim** // Jul 22, 2008 at 6:26 pm

  I actually tried the pen-and-paper method before checking if it wrote the keys out to SD. Great job, bushing. The applications should be endless.

- 4 **kylehav** // Jul 22, 2008 at 6:33 pm

  Wow, this is great.

  What are the 'unk' keys?

- 5 **SageChaozu** // Jul 22, 2008 at 6:35 pm

  Goo d Show, Bushing. I was glad that you made it write to SD because all of my pencils are upstairs (had grabbed it from channel).

- 6 **theorbtwo** // Jul 22, 2008 at 6:37 pm

  Or, for more information on what these keys are, instead of just warning people not to ask: http://hackmii.com/2008/04/keys-keys-keys

- 7 **Kaiman** // Jul 22, 2008 at 6:45 pm

  Once again amazed, bushing.

  Great job.

- 8 **Synangel** // Jul 22, 2008 at 6:58 pm

  So, are these the elusive Key.bin files? Or are they a new set?

- 9 **bubba** // Jul 22, 2008 at 7:18 pm

  thanks for this …

- 10 **Newbie** // Jul 22, 2008 at 8:32 pm

  Didn't work for me with twilight-hack-v0.1-alpha3a
  I did copy xyzzy.dol to SD as boot.dol.
  Proceeded with twilight hack as usual.
  Wii shows "Loading binary image…" and stays there forever.
  The router doesn't show any connection from Wii. Even IP address is released…

- 11 **Kaiman** // Jul 22, 2008 at 8:59 pm

  @Newbie: Twilight Hack 0.1alpha3a doesn't load .dol files. (see changelog at wiibrew to see for yourself)

  Upgrade to to 0.1beta1 or use HBC.

  Hope that helps.

- 12 **http://openid.aol.com/daegunlee** // Jul 22, 2008 at 11:12 pm

  Hi, I have a Korean version Wii and I want to extract the new key in Korean Wii. (I also have a Japanese version, too.)
  You've said that the Korean wii have two common keys. (known old one and unkown new Korean one)
  Is it possible to extract the new Korean key with this program?

- 13 **senti5000** // Jul 23, 2008 at 12:07 am

  You forgot the most important part of the code, but oh well…..

- 14 **marcan** // Jul 23, 2008 at 1:23 am

  Actually, 0.1alpha3a does support .dol files, but they have to be named boot.elf

  You should still update to 0.1beta1 though.

- 15 **bushing** // Jul 23, 2008 at 1:46 am

  @senti5000: ?

- 16 **w11h4x0r** // Jul 23, 2008 at 2:59 am

  so, can we erase pre-existing IOS versions now?
  when the system menu gets rebooted into the hack ios and the hack is bad, is the wii bricked? can we reboot/cut the power/revert to the original?
  your solution will work on other ios versions, right?

- 17 **https://me.yahoo.com/a/Nej4z1d6gZhv2QPT9ry3RkNcCPMknw--** // Jul 23, 2008 at 5:22 am

  Maybe senti5000 refers to the fact that in main() the check not to modify 1-1 seems to be missing. Only checks for 1-2 and 1-30 are implemented.

- 18 **Newbie** // Jul 23, 2008 at 6:53 am

  @Marcan

Do you mean if I copy xyzzy.dol to SD as boot.elf, it'll work?
Just don't want to brick my Wii.

Another thing, should we go ahead and download IOS11 from N site before they block it?

- 19 **Newbie** // Jul 23, 2008 at 6:55 am

  Oops, sorry just read 0.1beta1 tries to load boot.dol, and falls back to boot.elf if boot.dol is not found

- 20 **Newbie** // Jul 23, 2008 at 7:07 am

  @Marcan
  Thank a lot! It worked with 0.1beta1

- 21 **San** // Jul 23, 2008 at 7:11 am

  @Newbie
  why do you need your wii keys if you dont even know how to use the tp hack properly?!

  btw you cant brick your wii just by renaming files… 

- 22 **Team-Gx » xyzzy Released** // Jul 23, 2008 at 7:42 am

  [...] HackMii Download: [...]

- 23 **Damion** // Jul 23, 2008 at 9:12 am

  what is this for anyways?

- 24 **nukeee** // Jul 23, 2008 at 9:23 am

  If I can compile and run patchmii or this app i get a network -26 error when getting the nus object. Everything compiles ok.

  however if i run your compiled DOL everything works fine with no network errors.

  I thought was my network connection but now its clear its not.

  Are you running libogc from the cvs? as i'm just using the June libogc from the installer.

  I'd like to get this to compile and run. Any help would be great.

  Thanks,
  Nuke

- 25 **Arm the Homeless** // Jul 23, 2008 at 10:12 am

  Maybe you should read the xyzzy announcement again.
  It echos your Wii's keys into a .txt file on the root of the SD.

- 26 **adr990** // Jul 23, 2008 at 10:30 am

  Omg it choked me when it told:
  Hopes… fails… bricks frimware… bugs… etc xD

- 27 **Yoshi Party** // Jul 23, 2008 at 11:27 am

  Give a new statement about the exploit and when you are going to build a first ISO-Loader or at least releasing the exploit…

  this xyzzy seems to be nice…but it's useless for all non-developers and only another step to the iso-loader…why don't you just give us, what we want?

  The homebrew-scene made the psp so much popular…for wii it will be the same;)

- 28 **Louise** // Jul 23, 2008 at 1:46 pm

  Can hacking the IOS allow the ARM to be used for general purpose calculations?

  Or does using the ARM lock out using the PPC?

- 29 **kmeisthax** // Jul 23, 2008 at 3:22 pm

  @Louise: Yeah you can run your own code on the ARM, if you know how to sign an IOS and get it on the Wii.

P.S. Bushing your openid system is screwed, it sets the default nickname to be the OpenID capability sent by the website, a big security no-no I think

Also nice dig on Waninkoko.

- 30 **Louise** // Jul 23, 2008 at 4:21 pm

  @kmeisthax: I don't know anything about hacking hardware, so I would need a library to take care of the dirty low level stuff for me.

  What I would like is for the ARM and PPC to share the same memory space.

  Is that likely to happen, ot completely out of the question?

- 31 **homemdosaco2000** // Jul 23, 2008 at 9:14 pm

  @bushing: Well, I couldn't leave this post on the other thread (dear Nintendo), as it is closed for comments (for obvious reasons). And I didn't feel like e-mailing you because you get a little angry with that. I was wondering if you could post something about your impressions of working with nintendo's engineers, and how you think they feel about the 'scene', homebrew, working with you, etc. Not really interested in the bug, as I can't program anything beyond math algorithms. Hope you don't get mad about this. Best regards.

- 32 **Bent** // Jul 24, 2008 at 6:30 am

  When I try to run this using the twilight hack, it gets to the "Sending things to Earth…" part (or whatever it says) then the twilight hack appears to reboot continuously, getting the the same point in xyzzy each time. Any ideas why?

  Also, running it through the homebrew channel I can't get the http request to succeed, it says it fails every time (don't have the exact error message at the moment).

- 33 **bushing** // Jul 24, 2008 at 3:33 pm

  @w11h4x0r: The hacked version of IOS it loads is patched so that it can delete versions of IOS, yes. No, it will not harm your system if the process is interrupted — see my earlier article on PatchMii.

  @#17: 1-1 is boot2, which can't really be "deleted".

  @nukeee: Yeah, try a newer libogc — net_init now retries itself when it gets -26 (-EAGAIN).

  @ homemdosaco2000: I don't yet have anything to write about, but sure, I'll do a debrief when the dust settles.

  @Yoshi-Party: Fail.

- 34 **linkinworm-c98** // Jul 24, 2008 at 3:48 pm

  @yoshi-party
  LAMO yea the HOMEBREW scene, the homebrew scene on psp isnt backup loading, its real homebrew like custom prx's, programs like lua and such.

- 35 **Damion** // Jul 24, 2008 at 8:00 pm

  bushing why not just get a dev kit?

- 36 **cr08** // Jul 24, 2008 at 8:45 pm

  @Damion: A devkit won't do squat in a case like this. A devkit is only going to give you access to what nintendo will allow which is going to be restricted to the little sandbox they have designed into the Wii.

- 37 **bitflusher** // Jul 26, 2008 at 12:01 am

  it worked like a charm. i was surprised how fast the process was.
  i am now sticking my personal keys in a safe place incase my wii gets bricked (perhaps even printed inside my wii)

  thanx, i hope i never need them for unbricking

- 38 **I have several Questions... - WiiNewz Forums** // Sep 23, 2008 at 5:49 am

  [...] I would say don't bother it just makes life harder. 2. You might find this useful at some point: xyzzy and of course there is also Waninkoko – Wii Projects. Beware all this stuff has the potential to [...]

- 39 **Recent Links Tagged With "xyzzy" - JabberTags** // Sep 30, 2008 at 11:04 pm

  [...] public links >> xyzzy xyzzy Saved by claudial on Mon 29-9-2008 Comment on C++ Algorithms: next_permutation() by xyzzy Saved [...]

- 40 **Helwem** // Oct 30, 2008 at 1:34 pm

  no longer works, I guess because of the update of Nintendo accounts for a thank you very much for all your work, when a Xyzzy 1.1?

- 41 **senorclean** // Oct 30, 2008 at 4:18 pm

  I guess the copy of IOS11 on nintendo's servers was patched after the latest update – which would screw up the fake signing needed here.

  I suppose it may still be possible to do using a cIOS to install the patched IOS11 – and if the old copy of IOS11 was fetched from somewhere else (SD card?)

  Maybe Bushing can shed some light.

- 42 **naturesbane** // Nov 28, 2008 at 10:00 pm

  bushing: this program hangs after "sending to Earth" text.

  Please confirm if this is now non-functional. Is their a means to still get keys?

  System: 3.2U, cIOS36rev7,cIOS37rev3,cIOS51. (No other cIOSs installed, including cIOS247 or 2479.)

- 43 **naturesbane** // Nov 29, 2008 at 12:48 am

  regarding comment 42: delete or ignore. XYZZY v1.1 was functional for me. Must have been user error.

You must log in to post a comment.

- ## Search It!

  Search

- ## Recent Entries

  - Open-source USB Analyzer / 27C3 12.19
  - Developers, Developers, Developers! 11.6
  - Insert Startup Disc 9.22
  - The scope of Homebrew Channel 8.19
  - The USB2 Release 8.14
  - Theming the Homebrew Channel 8.11
  - HackMii Installer v0.7 7.26
  - System Menu 4.3 update 6.24
  - of homebrew and "trusted computing" / antipiracy 5.15
  - "Pandora's Xbox: The changing community of the modern console" 5.1

- ## Blogroll

  - iPhone Dev Team Blog
  - mist's blog
  - root labs
  - tmbinc's blog
  - Wiibrew wiki
  - xorloser's blog

close

Galleries
of
by