

Forum:[Hack Forums](#)

Thread: [\[TUTORIAL\]Reverse Engineering an Application](#)

0020 - October 23, 2012, 5:39 pm

Why would I want to do this?

There are many reasons why you would want to do this. Here are a few reasons: Seeing how an app works

- Modify the app to make it do as you please

- Fix bugs

Reverse engineering can be very satisfying. I think of it as a game of logic. You have to think like a processor would. Be very logical and literal.

Where can I get apps to reverse?

The way FairPlay protection works is by encrypting the binary. FairPlay can be defeated very easily with a jailbroken device. Due to the application being encrypted, you can't reverse engineer it. If you attempt to reverse it, you will only get a few subroutines only useful for seeing how the application is decrypted. We need the bulk of the code. To get a decrypted binary, just get any cracked IPA. For this example, I will use the popular game, "Plague Inc." I DO NOT CONDONE PIRACY. DO THIS AT YOUR OWN RISK.

I have my .IPA file. What now?

Once you have your .IPA file of the app of your choosing, change the ".ipa" to ".zip" and extract as shown below. (P.S. Pay very close attention, Grin, this step can be a bit confusing.)

[img]http://f.cl.ly/items/2l2X3X3n422p0n0G0i2v/Screen%20Shot%202012-10-23%20at%207.26.38%20PM.png[/img]

[img]http://f.cl.ly/items/2G0A2D1j1q1M420O301z/Screen%20Shot%202012-10-23%20at%207.27.54%20PM.png[/img]

Once you have extracted your .IPA file, we are looking for the actual binary of the application. A ".app" file is a folder. The path is as follows:

Code <EXTRACTED IPA>/Payload/<APP>.app/<binary>

In my case it would be:

Code Plague Inc/Payload/Plague Inc.app/Plague

However, if you are on OS X, like I am, you will need to right-click the .app and click "Show Package Contents" as shown below.

[img]http://f.cl.ly/items/040Y3t0x0Q1Z39422943/Screen%20Shot%202012-10-23%20at%207.29.47%20PM.png[/img]

Can we start reversing?

Yes; In fact we can. Go ahead and open up the binary we've located with IDA. Copy the settings in the pictures shown below.

[img]http://f.cl.ly/items/352I0H023P292D293N1f/Screen%20Shot%202012-10-23%20at%207.33.20%20PM.png[/img]

Click "Ok" to all the dialoge boxes that come up. Your screen should be similar to the one below.

[img]http://f.cl.ly/items/3P0o0s3Z3n091o0C252E/Screen%20Shot%202012-10-23%20at%207.35.51%20PM.png[/img]

IDA will analyze the binary we have opened. During this process, be patient; analyzing can take a while depending on the size of the binary.

After that, you are finished! Begin to go through interesting subroutines.

You are free to modify this binary and save it. You can then either repack the IPA or just put the .app on your device.

It might also be helpful if you have a ARM instruction set guide handy. Its a life saver.

If you have any questions, feel free to ask away here in this thread, or PM me. I'll try to get back to you as soon as possible.

Puller - October 23, 2012, 6:32 pm

Nice tut but I have a pdf on this already here <https://hackforums.net/showthread.php?tid=2930779>

0020 - October 23, 2012, 6:59 pm

Huh. Didn't know that PDF existed. Sorry about that.

Grin - October 23, 2012, 7:49 pm

Alright bud. Nice tutorial.

But i still do not agree that .zip = .ipa :)

0020 - October 23, 2012, 7:57 pm

An IPA is a ZIP. You can't deny that fact.

Grin - October 23, 2012, 10:31 pm

^The fuck? No...a zip is a zip. A zip is not a rar. lol

An ipa is not a zip.

0020 - October 24, 2012, 2:54 pm

An IPA is a zip file container. If this was not the case, nothing could be extracted using a zip extractor. I never said rar was a zip either.

Grin - October 24, 2012, 2:58 pm

...you said that ipa was a zip. So I made an analogy.

Rahul_Rulz - October 26, 2012, 1:36 pm

Can we know the resource of Application using this ?

I have a application which has got some really good wallpapers. I want to know where do they get them from and I want to download them all in bulk...so if I get thier FTP or webserver I would use third party download manager and download them all

Thank you for the guide I will test on some applications.

deprishy - October 26, 2012, 7:07 pm

(Oct 23, 2012 07:57 PM)0020 Wrote: [\[CITE\]](#) An IPA is a ZIP. You can't deny that fact. Denied.

That's not factual, and it's wrong.

An IPA is simply an archive for an iPhone application.

It actually is quite analogous to say a zip compression method is the same as a rar compression.

Grin - October 26, 2012, 7:10 pm

(Oct 26, 2012 07:07 PM)deprishy Wrote: [\[CITE\]](#) Denied.

That's not factual, and it's wrong.

An IPA is simply an archive for an iPhone application.

It actually is quite analogous to say a zip compression method is the same as a rar compression. Fucking thank you. Ohhh a +3 by S70N3R :)

0020 - October 26, 2012, 9:30 pm

Here is proof it is a ZIP.

Here is the ZIP header format:

[img]<http://f.cl.ly/items/0m0F3k0A3o160Z3t1H3T/Screen%20Shot%202012-10-26%20at%2011.13.25%20PM.png>[img]

Then look at this hex dump of an IPA I had handy

[img]<http://f.cl.ly/items/0V3p0R3l301t0q0k0t3R/Screen%20Shot%202012-10-26%20at%2011.14.03%20PM.png>[img]

Note those first four bytes. They are, 0x504B0304. Byte-flip it to get little endian and you get 0x04034B50.

Those first four bytes are the same in EVERY IPA. That pattern of values is unique to almost every ZIP file. There are a few exceptions.

Heres another example, according to the table, the four bytes at offset 30 (0x1E) defines the filename. Lets look at that! I have highlighted the hex in this picture.

[img]<http://f.cl.ly/items/451a2F1p3E0f2E1l0n3k/Screen%20Shot%202012-10-26%20at%2011.24.18%20PM.png>[img]

I think this is sufficient to say, that an IPA is actually a ZIP container.

I'm done with this skid bullshit.

Grin - *October 26, 2012, 9:32 pm*

A ZIP container...? So it's not a ZIP...it's a ZIP container.

MarkLeevE - *November 26, 2013, 8:50 am*

He's right, .ipa is just zipped compressed, there's no difference.

raymonf - *November 26, 2013, 6:37 pm*

A .ipa file is basically just a .zip file with a different file extension. But then again, it's not .zip. It's a compressed archive.. which is .zip in this case.

Yeah...

zip container != zip