Down the Drain

My journey into the pinball binaries.

Overview

After Blackhoodie I've been in a curiosity fueled binary fever. That fever combined with my new hobby of pinball has caused me to download the latest game binaries for the modern pinball machines to see what's inside.

Problems to solve

1. Figure out file format
2. Find interesting binaries
3. Learn a whole new disassembler
4. Choose a function to analyze

Project objective

This project really started out of curiosity solely. In the beginning, the main objective was to practice reversing and learn different techniques.

File Format

01

Stern’s game image file format is weird.

After downloading the image, I tried to find a utility to unpack their spk file. It seemed however someone had done this already, but Stern had taken it down.

File Format

02

If someone could do it, so could I:
So I took a look at the format.

Many of the files in the packed file were just bash scripts, so I came to some assumptions. It wasn’t compressed. It wasn’t encrypted. So I just found the patterns and wrote a python script to unpack it.

File Format

03

The script found a /usr dir, a /etc dir and a dir called iron_maiden_le.

From there I determined the binary that seemed most interesting was called “game”.

```
LE/iron_maiden_le/game: ELF 32-bit LSB executable, ARM, EABI5 version 1 (SYSV), dynamically
linked, interpreter /lib/ld-linux.so.3, for GNU/Linux 2.6.32,
BuildID[sha1]=f64ecb575a7f3aeb8ba74939bc1c65b5c5b16575, not stripped
```

Disassemble

04

I loaded up IDA with my findings.
The Arm processor type was not included with the free version of Ida.

I found radare2 as an alternative which did have arm support. Radare2 turns out to be much different then IDA and has a fairly steep learning curve.

So I found this GUI called cutter. This allowed to me to learn some of the techniques of labeling and viewing the code in a more intuitive way.

Choose a starting point

05

After staring at the output radare2 gave me, I decided to try and focus on one part of the code.

I decided to do something simple. I wanted to see if I could find some indication of where the code was talking to hardware. This turns out to be not that simple in modern games.

Hopefully I can sort of show you live the setup I have.

Other Pinball Software

I have a pinball machine at home. I would love to look at it's decompiled innards but it is an old Motorola chip (Motorola 68B09E).

I'm not sure IDA supports this, but certainly the free version does not.

Some Findings

The Stern pinball company doesn’t seem to care if I decompile their code. They don’t encrypt and I didn’t have to click through anysort of license agreement.

The code appears to be all there, but it’s large. This is a modern game with an LCD screen and modern sounds. The file I was decompiling was 5MBs.

Learning a new disassembler/assembly is non-trivial.

Thank you.

GERMANY
ITALY
ENGLAND
ARTIAN
TTACK
LTIBALL
TOTAL ANNIHILATION
CONQUER MARS
COMPLETE ALL 6
TO LIGHT
RULE THE UNIVERSE