CSI 2334 F19 Project

Section 02

Final Report

By Sam Hobbs & Jojo Cordova

Cynthia Fry

Due December 5, 2019

Summary of Activity

We first converted Tana1983.2334 to an executable through VirtualBox and learned that it started a mini game of snake in the console window, but on inputting a key, it displayed messages and initiated a malicious loop of continuously opening windows until it crashes the computer. Then, we uploaded the file in onlinedissassembler.com to gain a cursory understanding of the program, and Jojo used Ghidra to remove the call to mostImportant, which initiated the malicious loop. After that, Sam used Ghidra to modify the instruction code in the main function two implement two mods (as of 12/2/19): one which speeds up the game flow on increasing score and another which changes the snake’s mouth and makes the vertical and horizontal speed more consistent.

How We Approached the Problem (Tools & Techniques, (Dis)advantages)

We used onlinedisassembler.com and Ghidra to modify the source code and used GitHub to share. Jojo initially used VirtualBox once to test the program’s function apart from the main computer to ensure safety. Onlinedisassembler.com allowed us to gain a cursory understanding of a program’s general structure and calling code in the early phases of the project, but its code formatting (such as “lea 0x4(%rbp),%rax”) was difficult to understand, did not provide a decompilier, and did not allow for modifying the source code. Ghidra, on the other hand, allowed us to modify the source code and export as a new binary file in addition to analyzing the source code (with clearer formratting), and it even had a decompilier to allow us to see how it would run in C++ (though the decompilier is not completely accurate). On the downside, the interface made it somewhat difficult clearing bytes and modifying jump commands to allow modifications, but we suspect other disassemblers would have similar issues. Jojo used Ghidra to replace the malicious call to importantFunction with funkyFunc2 (which did nothing), and I used Ghidra to change several bytes to allow room for and implement my mods, such as increasing speed of the snake with the score and making the vertical speed consistent with the horizontal speed.

Explicit Mod Changes

Timeline

**Tuesday October 29, 2019 –** Tana1983.2334 is released.

**Thursday October 31, 2019 –** JoJo and Sam join together and create The Modders project group.

**Saturday November 2, 2019 –** First meeting, first report is delivered. Basic roles are established, first viewing of the code using *ODA – The Online Disassembler*.

**Monday November 4, 2019 –** *VirtualBox* is used to safely run the file in a controlled state and figure out its contents. It’s now confirmed that the executable is a game of “Snake” that when ran seems to be normal, but if any key is pressed then 3 messages will be displayed before 1000 windows will be opened. Each of these windows displays the message “YOU MADE A MISTAKE”.

**Tuesday November 5, 2019 –** Meeting with Cindy Fry. Second meeting in order to find where the malicious code is located. Location was not found but data strings were.

**Saturday November 9, 2019 –** *Ghidra* is first used. Malicious code is located.

**Sunday November 10, 2019 –** Malicious code is quarantined.

**Tuesday November 12, 2019 –** Second report is delivered.

**Wednesday November 13, 2019 –** Third meeting, mods are discussed along with roles.

**Monday November 18, 2019 –** Fourth meeting, basic mods are decided. Minor ones include changing game end messages and changing game visuals. Major includes changing game speed to increase as pellets are consumed, and change vertical speed to match the visuals of horizontal speed.

**Thursday November 21, 2019 –** Fifth meeting, roles for final section are delegated.

**Friday November 22, 2019 –** Work on final mods and final report begins.

**Monday November 25, 2019 –** Sixth meeting (over the phone), roles are re-delegated. Work on first major mod begins.

**Wednesday November 27, 2019 –** Sam completes the main mod: changing base game mechanics. The speed of the game increases as the pellets are consumed.

**Sunday December 1, 2019** – Sam completes second mod: changing base game mechanics. The snake’s head is changed from an arrow depending on direction to always a ‘0’, reduced vertical speed of snake to be physically closer to horizontal speed

**Monday December 2, 2019** – Sam begins work on the final report; seventh meeting between team members

Links:

<https://github.com/Fireman89/CS-Project>

<https://github.com/charger716/jazzHands>

https://onlinedisassembler.com/odaweb/AJhUQzTk