SAND2021-8312D

The Center for Cyber Defenders

Expanding computer security knowledge

Firmware Reverse Engineering

Utilizing Ghidra

Ryan Vaughan, Oklahoma State University

Project Mentor: Josh Templin

- Problem Statement:
  - Perform firmware reverse engineering on a commercial device about which little information is known
  - There are certain questions to answer about specific functionality of the device
  - Analyzing this binary poses additional challenges because it is a multiprocessor system with minimal documentation

- Objectives and Approach:
  - Search program space by using strings, instructions, and patterns
  - Compare results for each processor
  - Further map the space through function trees to locate functions which can answer the important questions

```
004010e8 e8 9c 05     CALL       _rand
         00 00
004010ed 03 c0        ADD        EAX,EAX
004010ef 83 f8 01     CMP        EAX,0x1
004010f2 0f 9c c0     SETL       AL
004010f5 89 3e        MOV        dword ptr [ESI],EDI
004010f7 83 c7 01     ADD        EDI,0x1
004010fa 88 46 24     MOV        byte ptr [ESI + 0x24],AL
004010fd 84 c0        TEST       AL,AL
004010ff b8 04 b2     MOV        EAX,s__likes_Cheese_0040b204
         40 00
00401104 75 05        JNZ        LAB_0040110b
00401106 b8 f4 b1     MOV        EAX,s__hates_Cheese_0040b1f4
         40 00
```

Example Disassembly

- Desired Results:
  - Understand the roles of different cores in a multiprocessor system
  - Use system context and understanding to identify and reverse functions of interest
  - Answer the specific questions about the desired binary

```
void __cdecl FUN_004010e0(int *param_1)

{
  bool bVar1;
  int iVar2;
  char *pcVar3;
  int iVar4;

  iVar4 = 0;
  do {
    iVar2 = _rand();
    bVar1 = iVar2 * 2 < 1;
    *param_1 = iVar4;
    iVar4 = iVar4 + 1;
    *(bool *)(param_1 + 9) = bVar1;
    pcVar3 = " likes Cheese";
    if (!bVar1) {
      pcVar3 = " hates Cheese";
    }
    _printf("%s %s\n",param_1 + 1,pcVar3);
    param_1 = (int *)param_1[10];
  } while (param_1 != (int *)0x0);
  return;
}
```

Example Decompiled Code

- Impact and Benefits:
  - By using Ghidra, we can answer critical questions that will enhance national security capabilities

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2017-XXXXC.

U.S. DEPARTMENT OF ENERGY | National Nuclear Security Administration

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.