Software Security via Program Analysis

Zombie Moon Buggy

Yu-Sheng Wang (bqk3dj)

Ignore Car Crash

1. By analyzing the source code, I find the function *crash_check* in *buggy.c*. The car will crash if the function return 1 when the car hit the gap.
2. Searching at *moon-buggy.S* with keyword "crash_check" and identify the anchor points.
   ```
   b004:   48 8b 05 9d 43 01 00     mov   0x1439d(%rip),%rax      # 1f3a8 <state>
   b030:   c3                       ret
   ```
3. Use PinTool function *INS_InsertDirectJump* to jump to 0xb030 (return 0) before 0xb004 (right after the program enters the function).

Ignore Meteor Crash - 1

1. Find the function *car_meteor_hit* in *buggy.c* and find anchor points:
   ```
   b094:   31 c0                    xor   %eax,%eax
   b111:   c3                       ret
   ```
2. Use PinTool function *INS_InsertDirectJump* to jump to 0xb111 (return 0) before 0xb094 (right after the program enters the function).
3. By doing so, the car does not crash when hit the meteor with its front.

Ignore Meteor Crash - 2

1. Find the function *metoer_car_hit* in *meteor.c* and find anchor points:
   ```
   bc42:   48 63 05 83 37 01 00     movslq 0x13783(%rip),%rax
   bda0:   45 31 ed                 xor   %r13d,%r13d
   ```
2. Use PinTool function *INS_InsertDirectJump* to jump to 0xbda0 before 0xbc42 (right after the program enters the function and store the values in stack).
3. By doing so, the car does not crash when landing on the ground from jumping.

Achieve High Scores in a Short Time

1. I find a function *adjust_score* in *game.c* which calculate the score values. I search the keyword and locate the following anchor points:
   score += val;
   ```
   94d4:   03 3d 52 5e 01 00        add   0x15e52(%rip),%edi      # 1f32c <score>
   ```
   Here, the score is read from local memory and add to the register %edi, which stores val.
2. Use PinTool function *INS_InsertCall* to modify the register value in %edi:

```
{
    fprintf(DBG_LOG, "[Real Execution] EAX: %lx\n", *regRAX); // read value
    *regRDI = 99999; // new value
}
```