Song
Spring 2015

CS 161
Computer Security

Discussion 5

Question 1 ***Fuzzing and Symbolic Execution*** **(20 min)**

In this problem, we will explore various approaches to systematically test a piece of code.

```
1
2  int foo(uint8_t bar, uint8_t baz)
3  {
4      int buf[500] = {0};
5      if ((bar + baz) % 3 == 2)
6      {
7          buf[(bar + baz) % 500] = 4;
8      }
9      if (bar > 250 && baz > 250)
10     {
11         return -1;
12     }
13     else if (bar > 10 && baz < 245)
14     {
15         if ((bar % 2 == 0) && (baz % 2 == 1))
16         {
17             return buf[bar + baz] + 3;
18         }
19         else if ((bar % 2 == 1) && (baz % 2 == 1))
20         {
21             return buf[bar + baz + 3];
22         }
23         else
24         {
25             return buf[bar + baz];
26         }
27     }
28     else
29     {
30         return bar + baz + 3;
31 }
```

Reminder: `uint8_t` is a 1-byte int.

(a) What is the minimum number of test cases required for line coverage?
(b) What is the minimum number of test cases required for branch coverage?
(c) What is the minimum number of test cases required for path coverage?
(d) If we used blackbox fuzzing, what is the probability that a randomly generated set of inputs for bar and baz will cause a buffer overflow?
(e) Write the formula for the values of bar and baz that would cause a buffer overflow.

Solution: (a) For line coverage, we want every line in the code executed. Thus, we need at least 5 test cases.
(b) For branch coverage, we want to execute every branch. Thus, we need at least 5 test cases.
(c) For path coverage, we want to execute every possible path in the code. Thus, we need at least 10 test cases.
(d) Notice that the overflow can only occur on line 21 and when `bar + baz + 3` >= 500 and `(bar % 2 == 1) && (baz % 2 == 1)` and `bar > 10 && baz < 245`. The only value of bar and baz that make all three conditionals true is bar = 255 and baz = 243. Since `uint8_t` are unsigned 8-bit integers, we see that there is a (1/256)*(1/256).
(e) We can AND the conditions specified in part d.

```
bar + baz + 3 >= 500 &&
(bar % 2 == 1) && (baz % 2 == 1) &&
bar > 10 && baz < 245.
```

A final note: do not hesitate to ask for help! Our office hours exist to help you. Please visit us if you have any questions or doubts about the material.