Nanyang Technological University

AY2021-2022 Semester 2

CE/CZ4067 SOFTWARE SECURITY

Tutorial 10: Combinatorial Testing and Symbolic Execution

```
1  void foo(int a, int b, int c) {
2    int x = 0, y = 0, z = 0;
3    if (a)
4      x = -2;
5    if (b < 5) {
6      if (!a && c) {
7        y = 1;
8        z = 2;
9      }
10   }
11   assert(x + y + z != 3);
12 }
```

Figure 1: A simple C program.

1. Consider the C program shown in Fig. 1. Suppose the input parameters "a", "b", and "c" take values from {0, 1}, {1,2,3}, and {0,1}, respectively.

   (a) Use the pairwise testing method to generate a minimal set of tests for the `foo` function. List the generated tests and explain your answer.

   (b) What is the branch coverage of your generated test suite?

2. Consider the C program shown in Fig. 1. Assume that all input parameters are symbolic variables, i.e., with symbolic values "A", "B", and "C".

   (a) Draw a symbolic execution tree for the given program.

   (b) How many symbolic paths does the `foo` function have?

(c) How many of the symbolic paths are feasible? List the path conditions of all feasible symbolic paths.

(d) Could the assertion on Line 12 ever be violated? If yes, what is the path condition that triggers the assertion violation? If no, explain your answer.