Lab Problems

Symbolic Execution

Ex.1

- Draw symbolic execution tree for this example (n is symbolic)

```
void test(int n) {
   int x=0;
   while(x<n)
      x=x+1;
}
```

Ex. 2

- Draw symbolic execution tree for this example. How many paths do you observe? Can you “repair” the program?.

```
void test(int x, int y, int d) {
   d=d+1;
   if(x>y)
      return d/(x-y);
   else
      return d/(y-x);
```

Ex. 3

- Draw all executions for the following code using **dynamic** symbolic execution; assume we only have decision procedure for **linear** constraints; start with **x=3** and **y=7**.

```
void test(int x, int y) {
   int z=x*x*x;//non-linear
   if(y==z)
      assert false;
}
```

Ex 4. Install Java PathFinder and Symbolic PathFinder

0. You need **java 8**.

1. download jpf-core (from SPF site) and jpf-symbc (e.g. in your home dir)

(both available from https://github.com/SymbolicPathFinder)

2. in your home dir create .jpf/site.properties

3. example site.properties:

    jpf-core = ${user.home}/Documents/workspace/jpf-core

    jpf-symbc = ${user.home}/Documents/workspace/jpf-symbc

    extensions = ${jpf-core},${jpf-symbc}

4. run jpf or spf

java -jar ~/jpf-core/build/RunJPF.jar MySUT.jpf

5. use eclipse (recommended)

6. see examples

Ex. 5

- Run "`oldclassic.jpf`" (see `jpf-core/src/examples`)

- How many paths do you observe?

Ex. 6

- Run examples from `jpf-symbc/src/examples/summerschool/`

- How many paths do you observe?

Ex. 8

- Consider the **`verifyPassword`** example; 4-bit input and password; D=256; how man steps are needed by the attacker to guess the full password? Please explain.

```
boolean verifyPass(byte[] input, byte[] password){
   for(int i=0;i<SIZE;i++){
      if(password[i]!=input[i])
         return false;
      Thread.sleep(25L);
   }
   return true;
}
```

Ex. 9

- Consider again the **`verifyPassword`** example; Compute Shannon Entropy (observable is time).

- Consider “corrected version” below; Compute Shannon Entropy.

```
boolean verifyPassC(byte[] input, byte[] password){
    boolean matched;
    for(int i=0;i<SIZE;i++){
        if(password[i]!=input[i])
            matched=false;
        else
            matched=matched;
        Thread.sleep(25L);
    }
    return matched;
}
```

Ex. 10

- Neural network example.
- Please watch video on NeuroSPF: https://www.youtube.com/watch?v=seal8fG78LI
- Download NeuroSPF: https://github.com/corinus/neurospf
- Run example: see src/examples/neurospf