Software Security & Secure Programming

Static Analysis - Exercises

Exercise 1.

We consider the following C program :

```
int main() {
   int x ;
   int tab[33] ;

   x = 1 ;
   while (x<24)
         x = x*2 ;
   tab[x] = 0 ;
   return 0 ;
}
```

1. Insert the assertion required to make this code "secure"
2. Draw its CFG
3. Run an interval-based VSA (without widening)
4. Are the assertion discharged ?
5. Is there a chance to discharge them using WP ?

Exercise 2.

We consider the following C program :

```
void compute (int x, int y) {
  int z, u;
  u = x ;
  z = 0 ;
  while (z<y) {
    z = z+1 ;
    u = u+1 ;
  }
  return u;
}

int main() {
   int a ;
   a = compute (5, 3) ;
   tab[a] = 0 ;
   return 0 ;
}
```

1. Insert the assertion required to make this code "secure"
2. Draw the CFG of function `compute` (assuming initial value of `x` and `y` are 5 and 3).
3. Run an interval-based VSA over function `compute` :
   (a) without norrowing
   (b) with narrowing
4. Are the assertion discharged ?
5. Add a specification (as a pre/post-condition) for function `compute`
6. Run the VSA again using this assertion. Are the assertions now discharged ?
7. Prove the specification of function "compute"