Software Security
Practical Task 01

Sven Schäge

Practical Software Analysis

- Open the C program here:
  https://techiedelight.com/compiler/?SoftSec_PassChecker
- Make yourself familar with the editor (running code is triggered via the green button).
- The program is a modified version of the program given in the lecture slides. Its purpose is to check for Alice password.
- Run the program with input 123456789.
- Run it with input 1234567890.
- Run it with input 12345678901.
- Explain the behaviour. To this end describe the underlying security weakness that this program features and propose security fixes.

Fx Measure

- Assume we value recall twice as high as precision.
- Assume we have two code analysers A1 and A2 that both check if a given program is free of use-after-free-bugs.
  - A1 has precision of 50% but high recall of 90%.
  - A2 has a precision of 70% and recall of 80%.
- Which of the analysers has a better Fx measure? Compute both FX measures and compare!

Generate the CFG

```
x = 3;
y = 3;
z = 5;
while (z == 5) {
  if (x != 3) { y = 0;} else { y = 1; };
  while (y*z != 0) {
    y=y-1;
  }
}
```