CSC 347 - Concepts of Programming Languages

Undefined Behavior

Instructor: Stefan Mitsch

Learning Objectives

❓ What should happen if the language does not specify the meaning of some construct?

❓ What should happen when `x` is holding 8 bits, `x=7` and then `x = x+1`?

- Understand examples of undefined behavior in C

Under and Overflow

```c
#include <stdio.h>

int isMinValue (int x) {
  return (x-1) > x;
}
int main () {
  int i = -2000000000;
  while (!isMinValue(i))
    i--;
  printf ("Min value is %d\n", i);
}
```

```
$ gcc -O1 undefined.c && ./a.out
Min value is -2147483648
```

```
$ gcc -O2 undefined.c && ./a.out
^C #infinite loop
```

Order of Operations

```c
#include <stdio.h>
int count = 0;
int f () {
  count += 1;
  return count;
}
int main () {
  int z = f() + f();
  printf ("%d\n", z);
  z = (z += 1) + (z = z*z);
  printf ("%d\n", z);
}
```

```
$ clang -Wall undefined3.c
undefined3.c:11:21: warning: unsequenced modification and access to 'z'
  z = (z += 1) + (z = z*z);
         ~~     ^
1 warning generated.
$ ./a.out
3
20
```

- `z=z+1; z=z+z*z`

Order of Operations

```c
#include <stdio.h>
int count = 0;
int f () {
  count += 1;
  return count;
}
int main () {
  int z = f() + f();
  printf ("%d\n", z);
  z = (z += 1) + (z = z*z);
  printf ("%d\n", z);
}
```

```
$ gcc -Wall -O3 undefined3.c
undefined3.c: In function ‘main’:
undefined3.c:11:5: warning: operation on ‘z’ may be undefined
   z = (z += 1) + (z = z*z);
     ^
$ ./a.out
3
32
```

- `z=z+1; z=z*z; z=z+z;`

Compiler Optimizations

- For undefined executions, the compiler can do what it likes
- This can lead to some surprising compiler optimizations
- C null pointer optimization 1
- Discussion
- Discussion
- C null pointer optimization 2
- Haskell Optimization

Dangling Pointers

- See the worksheet for this week.
- More examples of undefined behavior
- More undefined behavior

Summary

- Undefined behavior resolved in the compiler (compiler decides what is the meaning of undefined programs)
- Undefined behavior often presents security risks