# Homework #3 for CS 419— Computer Security

## 1 Hardware Security (10 points)

Read the following side channel attacks on hardware and summarize them:

Row hammer: `https://en.wikipedia.org/wiki/Row_hammer`

Meltdown and Spectre: `https://meltdownattack.com/`

## 2 Integer overflow (10 points)

Lecture slides 14, for pages 52, 53, 54 and 55: please explain what will happen and why.

## 3 Format string attack (10 points)

Please use `printf` function as one example to demonstrate how to use different format strings to perform format string attack. At least you should use `%s` and `%n`. Please provide concrete example code and attack string.

## 4 Stack overflow (30 points)

Modern OS tries to prevent basic stack overflow attacks. Let us try to perform stack overflow attack. For the following program,

```
void execcmd(char *str) {
    char buf[128];
    strcpy(buf, str);
    system(buf);
}
```

Please write in details:

- All the necessary (compiler and OS) options/configurations you need to do to make the attack happen in a modern OS, 64 bit Ubuntu 18.04.4 LTS (Bionic Beaver); (5 points)
- Your attack input and effects; (5 points)

- Dump your program code in assembly and for each each instruction, draw the call stack (using the attack string as input); (15 points)
- Explain why you cannot perform the attacks without these options/configurations. (5 points)

## 5 System Audit (10 points)

There are many ways of solving the dependence explosion problem to improve provenance analysis. Please think of a few ideas of how to do this and explain why using the example on page 37 in slides 15.