CSE 484 In-Class Worksheet #20 – Autumn 2018

Name: _____ UWNetID: _____ Date: _____

Email address: _____

Partner names for this activity: _____

Will you want to pick up your worksheet later? Circle one: Yes / No

Q1: Consider this code, running as a kernel system call or as part of a cryptographic library.

```
if (x < array1_size)
        y = array2[array1[x] * 256];
```

Suppose:

- That an adversary can run code, in the same process.
- That an adversary can control the value x.
- That an adversary has access to array2.
- That the adversary's code cannot just read arbitrary memory in the process.
- That there is some secret value, elsewhere in the process, that the adversary would like to learn.

Can you envision a way that an adversary could use their own code, to call a vulnerable function with the above code, to learn the secret information? Leverage branch prediction and cache structure / timing.

Q2: What other side channels might exist? How might an adversary use them?