UNC CHARLOTTE

College of Computing and Informatics

Department of Software and Information Systems

Enterprise and Infrastructure Protection
ITIS 6230

# PROJECT 2 – SPECTRE: STEALING SENSITIVE INFORMATION WITH CACHE

SAHIL BHIRUD

**(1)**

**Access Delay Time to array[i*4096]**

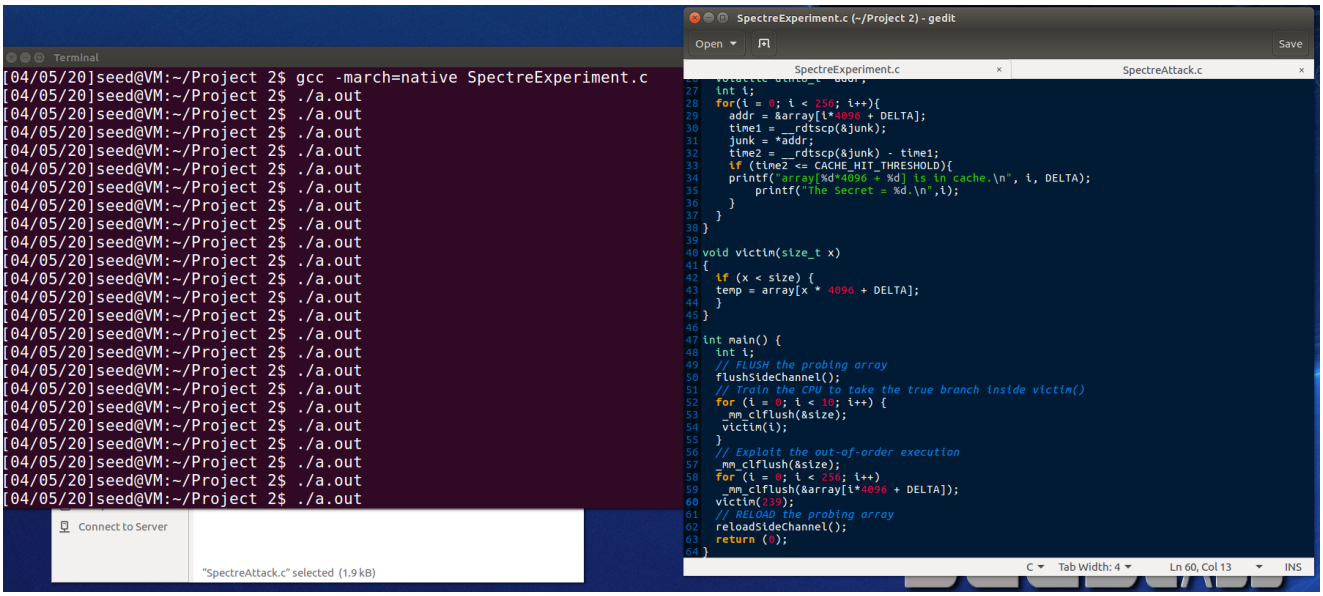
| array[i*4096] where i= | Average (CPU cycles) |
|---|---|
| 0 | 1799 |
| 1 | 281 |
| 2 | 281 |
| **3** | **134** |
| 4 | 278 |
| 5 | 280 |
| 6 | 358 |
| **7** | **129** |
| 8 | 298 |
| 9 | 298 |

**(2)**

**Access Delay Time to the secret**

| Execution 1 | Execution 2 | Execution 3 | Execution 4 | Execution 5 | Execution 6 | Execution 7 | Execution 8 | Execution 9 | Execution 10 | Average |
|---|---|---|---|---|---|---|---|---|---|---|
| 72 | 72 | 78 | 58 | 76 | 76 | 80 | 70 | 70 | 78 | **73** |

**(3)**



To come to this conclusion, I recursively complied and ran the program after augmenting the parameters passed to the victim() function.

**(4)** The secret is guarded by the sandbox function which divides the memory in two sections viz. Restricted and Unrestricted. We need to manipulate the CPU to execute an out-of-order execution in order to recover the secret from the restricted area. This done by speculative execution. Speculative execution is an optimization technique in which the processors or the CPU performs some task that may not be needed. If the work is not needed then, the changes are reverted, and the results are ignored. This may leave observable side effects that may reveal private data to attackers.

So, by flushing the buffer_size and using out-of-order execution, the attacker tries to delay the execution as it will take some time for the CPU to fetch data from the main memory and this is when the attacker will obtain the secret from the restricted area.