

Part 1.1

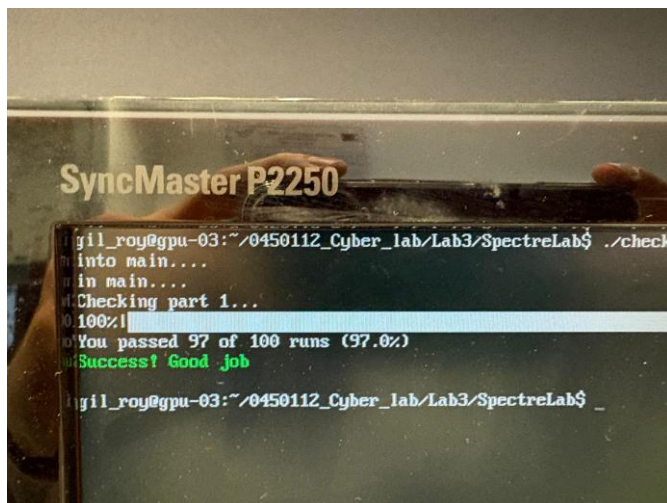
Cache time

L1	L2	DRAM
20	40	400

1.2

The secret data type is char, can obtain the value 0-255. Therefore need to evict 256 pages from the TLB.

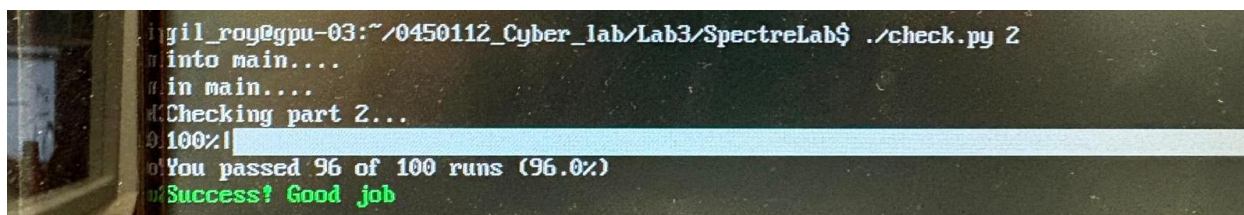
1.3 picture



Part 2.1

The code won't work since our offset can't be larger than 3. the code might work in some specific situations where the secret code length doesn't exceed 4 bytes.

2.2 picture



2.3

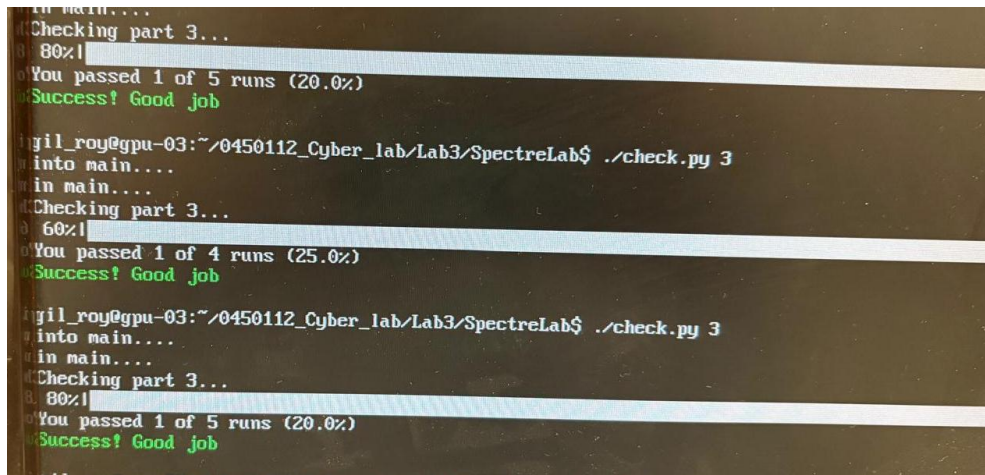
The attacker can use the same procedure without stopping in \0 then translate the data to

the relevant types. The attacker needs to know whether the system works in big or little endian.

2.4

We started from 2048 then used binary search to find the optimal value of 196.

Part 3.1



```
in main....
Checking part 3...
80%|
You passed 1 of 5 runs (20.0%)
Success! Good job

gil_roy@gpu-03:~/0450112_Cyber_lab/Lab3/SpectreLab$ ./check.py 3
into main....
in main....
Checking part 3...
60%|
You passed 1 of 4 runs (25.0%)
Success! Good job

gil_roy@gpu-03:~/0450112_Cyber_lab/Lab3/SpectreLab$ ./check.py 3
into main....
in main....
Checking part 3...
80%|
You passed 1 of 5 runs (20.0%)
Success! Good job
```

3.2

Our strategy was to rely on statistics as we ran 20 iterations and chose the most common. In addition we flushed the whole cache to extend the window of the missprediction.

3.3

Key Information Needed:

- Cache Architecture Details about the size and latency of L1, L2, as well as cache line sizes. This determines the timing differences critical for Flush+Reload.
- Branch Predictor Behavior: The specifics of how the branch predictor works, especially the history depth and whether predictors are shared between privilege levels.
- TLB Latency: TLB sizes, latency for TLB misses.
- Instruction Pipeline out of order: Information about speculative execution windows.

Yes, most of this information can be determined experimentally:

- Cache latencies and sizes can be measured using timing-based cache attacks like Flush+Reload.
- Branch predictor behavior can be inferred by repeatedly training and probing speculative execution patterns.
- TLB latencies can be measured by timing page accesses after triggering a TLB flush