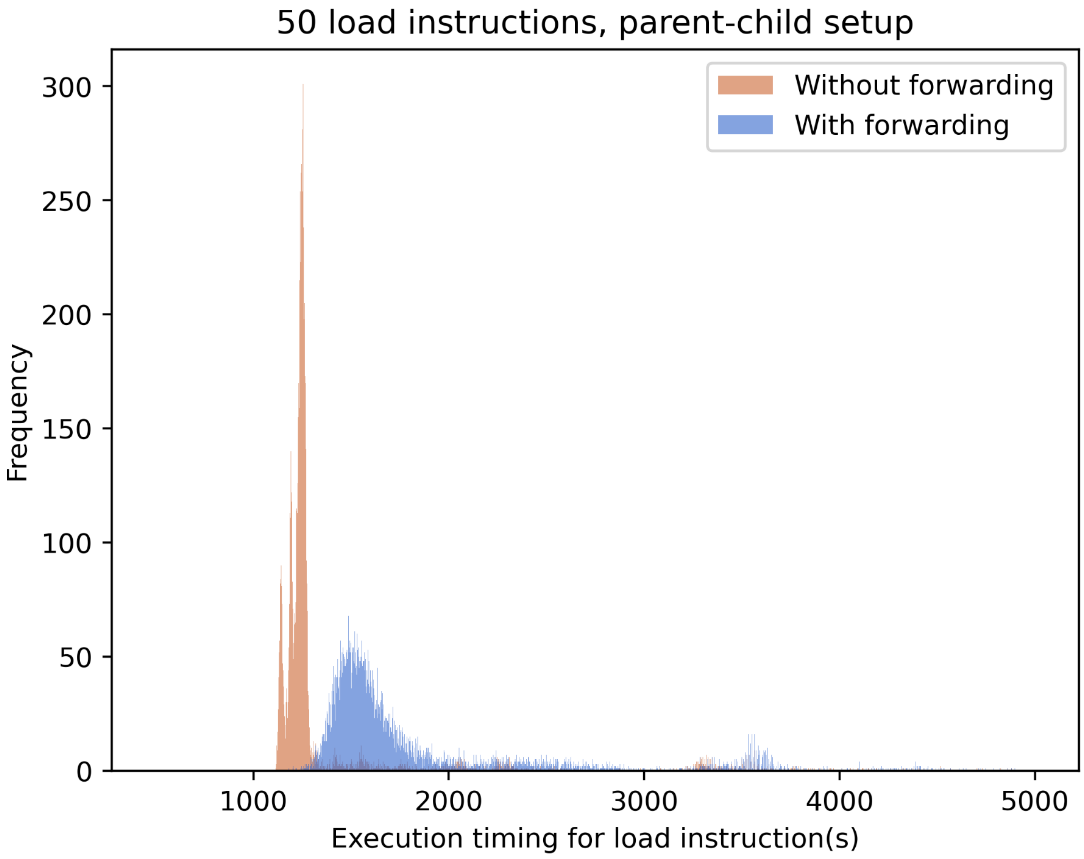
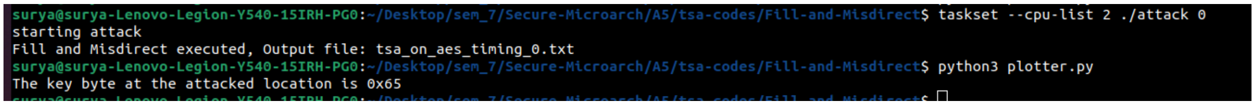
Secure Processor MicroArchitecture
Assignment 5 - Timed Speculation Attacks

Surya Prasad S - EE19B121

1. Plot generated by Fill and Forward strategy

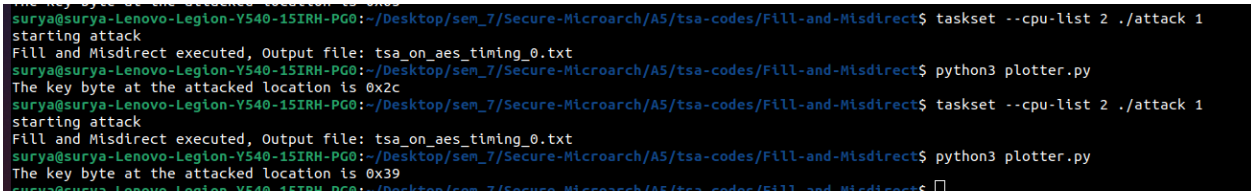


2. Fill and Misdirect strategy results: Only Key0 was identified properly
   Main key: 65 ff 32 54 44 bd 66 77 88 99 aa bb cc dd ee ff
   Key0:



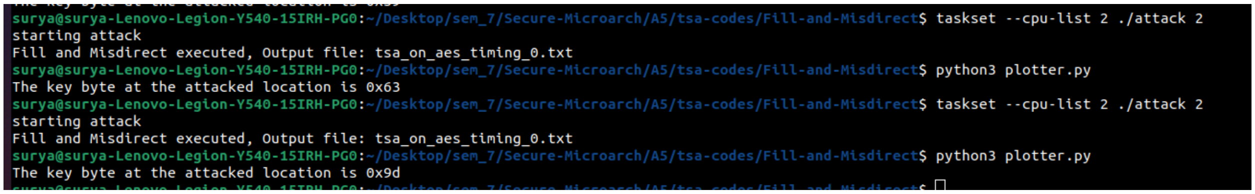
```
surya@surya-Lenovo-Legion-Y540-15IRH-PG0:~/Desktop/sem_7/Secure-Microarch/A5/tsa-codes/Fill-and-Misdirect$ taskset --cpu-list 2 ./attack 0
starting attack
Fill and Misdirect executed, Output file: tsa_on_aes_timing_0.txt
surya@surya-Lenovo-Legion-Y540-15IRH-PG0:~/Desktop/sem_7/Secure-Microarch/A5/tsa-codes/Fill-and-Misdirect$ python3 plotter.py
The key byte at the attacked location is 0x65
```

   Key1:



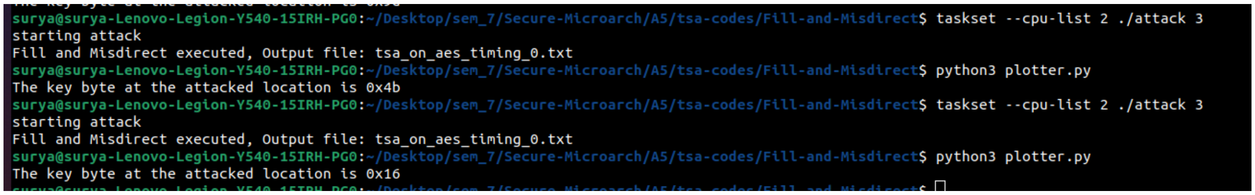
```
surya@surya-Lenovo-Legion-Y540-15IRH-PG0:~/Desktop/sem_7/Secure-Microarch/A5/tsa-codes/Fill-and-Misdirect$ taskset --cpu-list 2 ./attack 1
starting attack
Fill and Misdirect executed, Output file: tsa_on_aes_timing_0.txt
surya@surya-Lenovo-Legion-Y540-15IRH-PG0:~/Desktop/sem_7/Secure-Microarch/A5/tsa-codes/Fill-and-Misdirect$ python3 plotter.py
The key byte at the attacked location is 0x2c
surya@surya-Lenovo-Legion-Y540-15IRH-PG0:~/Desktop/sem_7/Secure-Microarch/A5/tsa-codes/Fill-and-Misdirect$ taskset --cpu-list 2 ./attack 1
starting attack
Fill and Misdirect executed, Output file: tsa_on_aes_timing_0.txt
surya@surya-Lenovo-Legion-Y540-15IRH-PG0:~/Desktop/sem_7/Secure-Microarch/A5/tsa-codes/Fill-and-Misdirect$ python3 plotter.py
The key byte at the attacked location is 0x39
```

   Key2:



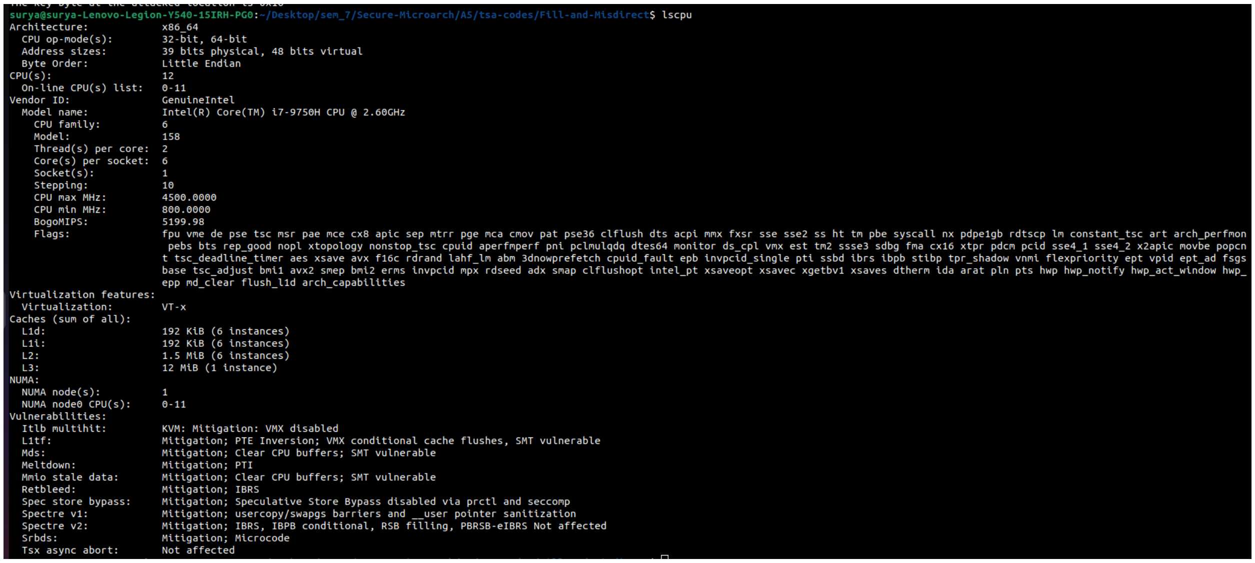
```
surya@surya-Lenovo-Legion-Y540-15IRH-PG0:~/Desktop/sem_7/Secure-Microarch/A5/tsa-codes/Fill-and-Misdirect$ taskset --cpu-list 2 ./attack 2
starting attack
Fill and Misdirect executed, Output file: tsa_on_aes_timing_0.txt
surya@surya-Lenovo-Legion-Y540-15IRH-PG0:~/Desktop/sem_7/Secure-Microarch/A5/tsa-codes/Fill-and-Misdirect$ python3 plotter.py
The key byte at the attacked location is 0x63
surya@surya-Lenovo-Legion-Y540-15IRH-PG0:~/Desktop/sem_7/Secure-Microarch/A5/tsa-codes/Fill-and-Misdirect$ taskset --cpu-list 2 ./attack 2
starting attack
Fill and Misdirect executed, Output file: tsa_on_aes_timing_0.txt
surya@surya-Lenovo-Legion-Y540-15IRH-PG0:~/Desktop/sem_7/Secure-Microarch/A5/tsa-codes/Fill-and-Misdirect$ python3 plotter.py
The key byte at the attacked location is 0x9d
```

Key3:



```
surya@surya-Lenovo-Legion-Y540-15IRH-PG0:~/Desktop/sem_7/Secure-Microarch/A5/tsa-codes/Fill-and-Misdirect$ taskset --cpu-list 2 ./attack 3
starting attack
Fill and Misdirect executed, Output file: tsa_on_aes_timing_0.txt
surya@surya-Lenovo-Legion-Y540-15IRH-PG0:~/Desktop/sem_7/Secure-Microarch/A5/tsa-codes/Fill-and-Misdirect$ python3 plotter.py
The key byte at the attacked location is 0x4b
surya@surya-Lenovo-Legion-Y540-15IRH-PG0:~/Desktop/sem_7/Secure-Microarch/A5/tsa-codes/Fill-and-Misdirect$ taskset --cpu-list 2 ./attack 3
starting attack
Fill and Misdirect executed, Output file: tsa_on_aes_timing_0.txt
surya@surya-Lenovo-Legion-Y540-15IRH-PG0:~/Desktop/sem_7/Secure-Microarch/A5/tsa-codes/Fill-and-Misdirect$ python3 plotter.py
The key byte at the attacked location is 0x16
```

3. Output of lscpu



```
surya@surya-Lenovo-Legion-Y540-15IRH-PG0:~/Desktop/sem_7/Secure-Microarch/A5/tsa-codes/Fill-and-Misdirect$ lscpu
Architecture:            x86_64
  CPU op-mode(s):        32-bit, 64-bit
  Address sizes:         39 bits physical, 48 bits virtual
  Byte Order:            Little Endian
CPU(s):                  12
  On-line CPU(s) list:   0-11
Vendor ID:               GenuineIntel
  Model name:            Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz
    CPU family:          6
    Model:               158
    Thread(s) per core:  2
    Core(s) per socket:  6
    Socket(s):           1
    Stepping:            10
    CPU max MHz:         4500.0000
    CPU min MHz:         800.0000
    BogoMIPS:            5199.98
    Flags:               fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm pbe syscall nx pdpe1gb rdtscp lm constant_tsc art arch_perfmon
                          pebs bts rep_good nopl xtopology nonstop_tsc cpuid aperfmperf pni pclmulqdq dtes64 monitor ds_cpl vmx est tm2 ssse3 sdbg fma cx16 xtpr pdcm pcid sse4_1 sse4_2 x2apic movbe popcn
                         t tsc_deadline_timer aes xsave avx f16c rdrand lahf_lm abm 3dnowprefetch cpuid_fault epb invpcid_single pti ssbd ibrs ibpb stibp tpr_shadow vnmi flexpriority ept vpid ept_ad fsgs
                         base tsc_adjust bmi1 avx2 smep bmi2 erms invpcid mpx rdseed adx smap clflushopt intel_pt xsaveopt xsavec xgetbv1 xsaves dtherm ida arat pln pts hwp hwp_notify hwp_act_window hwp_
                         epp md_clear flush_l1d arch_capabilities
Virtualization features:
  Virtualization:        VT-x
Caches (sum of all):
  L1d:                   192 KiB (6 instances)
  L1i:                   192 KiB (6 instances)
  L2:                    1.5 MiB (6 instances)
  L3:                    12 MiB (1 instance)
NUMA:
  NUMA node(s):          1
  NUMA node0 CPU(s):     0-11
Vulnerabilities:
  Itlb multihit:         KVM: Mitigation: VMX disabled
  L1tf:                  Mitigation; PTE Inversion; VMX conditional cache flushes, SMT vulnerable
  Mds:                   Mitigation; Clear CPU buffers; SMT vulnerable
  Meltdown:              Mitigation; PTI
  Mmio stale data:       Mitigation; Clear CPU buffers; SMT vulnerable
  Retbleed:              Mitigation; IBRS
  Spec store bypass:     Mitigation; Speculative Store Bypass disabled via prctl and seccomp
  Spectre v1:            Mitigation; usercopy/swapgs barriers and __user pointer sanitization
  Spectre v2:            Mitigation; IBRS, IBPB conditional, RSB filling, PBRSB-eIBRS Not affected
  Srbds:                 Mitigation; Microcode
  Tsx async abort:       Not affected
```

4. Output of uname -a
Linux surya-Lenovo-Legion-Y540-15IRH-PG0 5.15.0-52-generic #58-Ubuntu SMP Thu Oct 13 08:03:55 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux