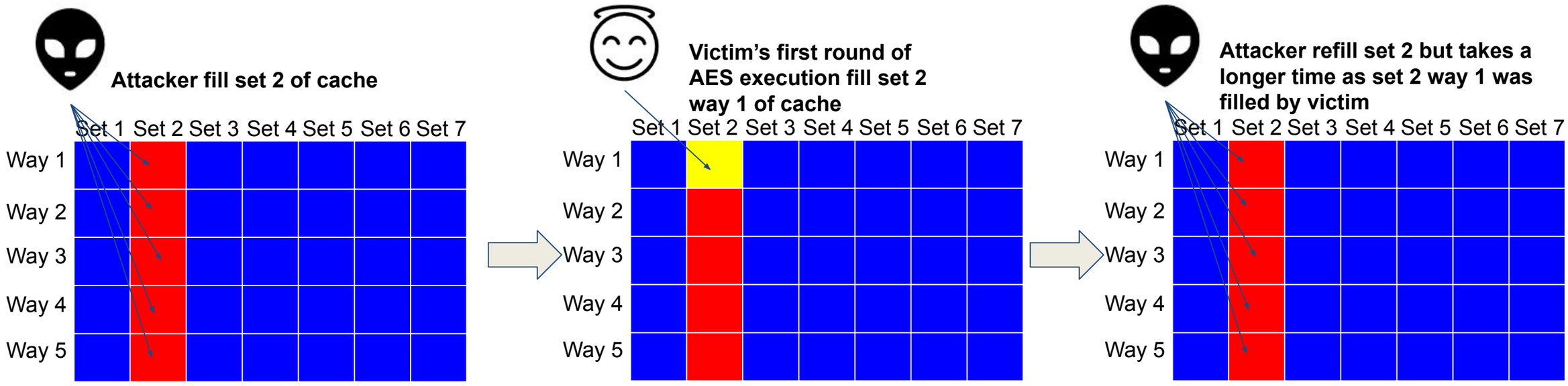
NANYANG TECHNOLOGICAL UNIVERSITY
SINGAPORE

School of Computer Science and Engineering
College of Engineering

Cache Attacks

Practical implementations on Intel's and ARM's core

Student: Benjamin Loh Wen Qian Supervisor: Dr Li Fang



A simple Prime and Probe attack Illustration

Project Objectives:

The project aims to develop cache attacks on the Intel® Core™ i7-7500U Processor and the Raspberry Pi 3B+, ARM v8A Cortex-A53 Processor and show the applicability to recover the first nibble of the 16-byte keys of a 128-bit Advanced Encryption Standard implemented with T-Tables. The development of these cache attacks in a realistic environment serves as a venue to further understand the workings of each side-channel attack and the applicability of the attacks on these platforms. The attack on the Intel CPU reflects an attack on a cloud computing platform while an attack on the ARM CPU reflects an attack on mobile devices.

List of Attacks:

<u>Intel Core:</u>

Prime and Probe (L1 and Last-Level-Core)
Flush and Reload
Evict and Reload

<u>ARM Core:</u>
Evict and Reload

```
counts_array 13 : 67525
counts_array 14 : 83152
counts_array 15 : 64587
k_firstbit 1
actual key 15
Terminated
counts_array 0 : 65464
counts_array 1 : 51164
counts_array 2 : 53636
counts_array 3 : 51552
counts_array 4 : 52739
counts_array 5 : 51843
counts_array 6 : 53215
counts_array 7 : 53621
counts_array 8 : 54928
counts_array 9 : 52772
counts_array 10 : 51973
counts_array 11 : 52646
counts_array 12 : 43222
counts_array 13 : 66943
counts_array 14 : 63919
counts_array 15 : 79880
k_firstbit 1
actual key 16
Terminated
```

Live Attack Example