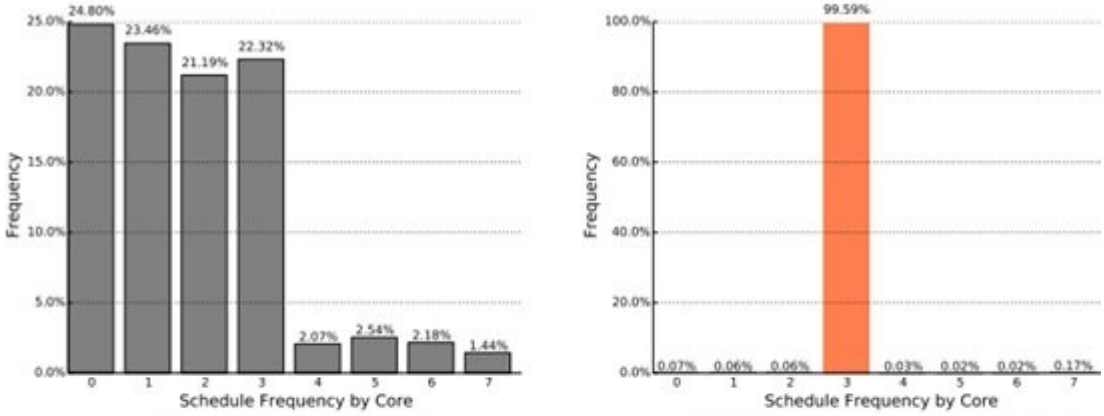
[illegible] ASLR [illegible]

[illegible] Branch Target Buffer [illegible] (BTB) [illegible] BTB [illegible]. [illegible] ALSR ([illegible] Address Space Layout Randomization) [illegible] [illegible] [illegible]

[□□□□□ □□□ □□□□□□ □□ □□□□□ □□□□□ □□□□□ □□ □□□□□□ □□□ □□□□ **10** □□ □□□□□]

□□□□□ □□ □ □□□□□ □□□□□□□ □□□□□ □□ □□□□ □□ □□□□□□□□□□□□□ □□ □□□□□□ □□□ □□ □□□□ □□□ □□ □□□□ □□□ □□ □□□□□ □□□□□□□ □□□□□ □□ □□□□ □□□□ □□□□□ □□□□□ □□□□□□ □□ □□□□□□ □□□□ □□ □□□□ □□□□ □□□ □□ □□□□□ □□ □□□□□□□ □□□□ □□ □□□□ □□□□ □□□□□ □□□□□ □□□□□□ □□ □□□□□ □□□ □□ □□



(a) No scheduling manipulation

(b) The spy forces scheduling at core number 3

Fig. 10: Scheduling of the victim process to virtual cores.

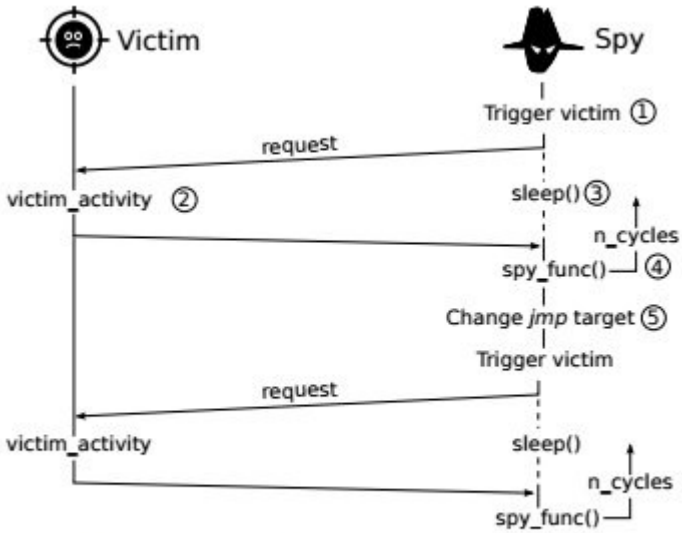


Fig. 8: Stages of the user ASLR attack

[illegible]:

[illegible] ASLR [illegible] BTB [illegible] BTB [illegible] BTB [illegible] BTB [illegible] (collision attacks) [illegible]. [illegible] ASLR [illegible]. [illegible] [illegible] [illegible]

□□□□□ □□□□□□□□
□□□□ □□□□:
□□□□□
□□□□□ □□□□□□:
09:17 - 10/08/1395
:□□□□□
□□□□□ □□□□ - ALSR - BTB - collision attacks - □□□□ □□□□□ - □□□□□ - □□□□□ - □□□□□□□□□ - □□□□ - □□□□□

□□□□□ □□□□: https://www.shabakeh-mag.com/security/5186