

[illegible][illegible]

The figure shows the results of the BTB-based attack on User-level ASLR. The x-axis represents the randomized part of the instruction address, ranging from 7efebe3e8 to 7efebe514. The y-axis represents the cycles to execute the spy's code block, ranging from 75 to 120. Two data series are plotted: T1 (blue dots) and T2 (green dots). T1 shows a significant spike at the target address 0x7efebe45a82, reaching approximately 118 cycles. T2 remains relatively flat, around 80 cycles. The target address is marked with a red 'X' and labeled '0x7efebe45a82'.

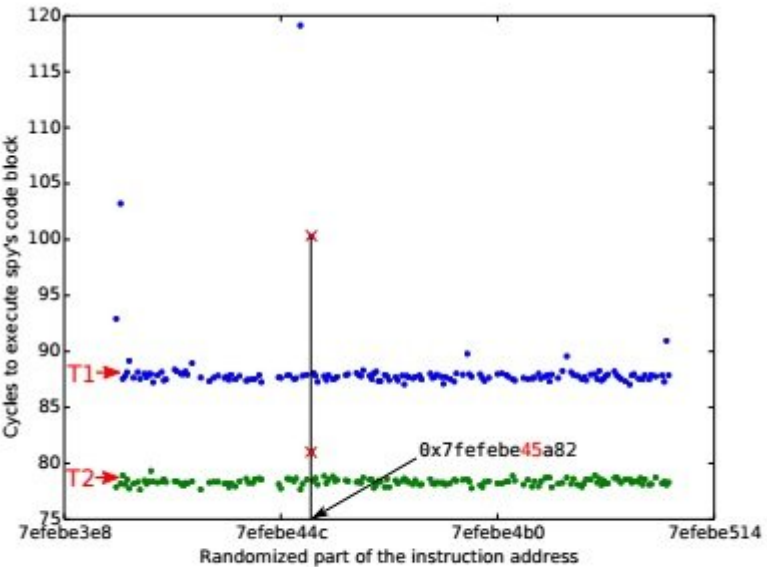


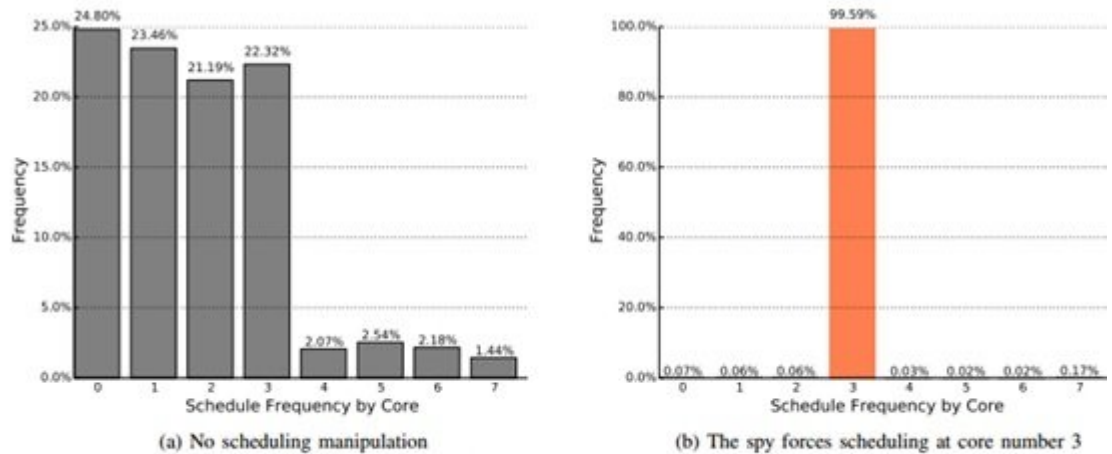
Fig. 11: Results of the BTB-based Attack on User-level ASLR

The figure shows the results of the BTB-based attack on User-level ASLR.

The x-axis represents the randomized part of the instruction address, ranging from 7efebe3e8 to 7efebe514. The y-axis represents the cycles to execute the spy's code block, ranging from 75 to 120. Two data series are plotted: T1 (blue dots) and T2 (green dots). T1 shows a significant spike at the target address 0x7efebe45a82, reaching approximately 118 cycles. T2 remains relatively flat, around 80 cycles. The target address is marked with a red 'X' and labeled '0x7efebe45a82'.

BTB-based Attack on User-level ASLR

"ASLR [1] is a technique that randomizes the memory addresses of executables and libraries. This randomization makes it difficult for an attacker to predict the location of specific code blocks or data structures. In this paper, we propose a BTB-based attack on User-level ASLR. The BTB (Branch Target Buffer) is a hardware structure that stores the targets of branches. By manipulating the BTB, an attacker can predict the next instruction address. This attack can be used to bypass ASLR and execute arbitrary code. The results of the attack are shown in Figure 11. The x-axis represents the randomized part of the instruction address, ranging from 7efebe3e8 to 7efebe514. The y-axis represents the cycles to execute the spy's code block, ranging from 75 to 120. Two data series are plotted: T1 (blue dots) and T2 (green dots). T1 shows a significant spike at the target address 0x7efebe45a82, reaching approximately 118 cycles. T2 remains relatively flat, around 80 cycles. The target address is marked with a red 'X' and labeled '0x7efebe45a82'.

[illegible]

0000 000 000000 000000 0000 00 000 000000 00 00 0000 00000 000 00 0000000 00 00 000000 00000 0000 0000
 .000000 000000 000000000000 60 00 0000 ASLR 00000000 0000000000 0000 0000 0000000 00 0000 00 000000 0000
 0000 000 00000 00000000000 00 00000 0000 00 000 00000 00000000 0000000000 00 00000 0000 00000000000 0000
 00 0000000000 000000 0000000000 .000000 00000000 000000 000000 0000000000 00 00000 00 000000000 0000000000
 .00000 00000000 00 0000 00000 000000000000000000 0000 00000 0000 000000000000 00000000000 000000 000000 0000 00
 000000000 0000000000000000000000 000000 00000 00 (Kernel Virtual Machines) 0000000 00000000000 00000 0000 00 0000000
 00000000000 0000 00 00 00 0000000 000000 00000 0000 00000 0000 0000000 0000 00 0000000 0000000000 00 000000
 0000000000 00 0000 0000 0000 00000 00000 00 0000000000 00000 00000000 0000000000 0000000000 0000000000 000000 0000
 0000 00 00000 000000000000 00000000 000000 0000 0000 00 00000 0000 0000 0000 00 ASLR 0000000000 0000000000 00000000000000
 .000000 000000000000 0000 00 00000000

:

موضوع: امنیت

موضوع: امنیت

موضوع: امنیت

موضوع: امنیت

09:17 - 10/08/1395

موضوع: امنیت

موضوع: امنیت - ALSR - BTB - collision attacks - موضوع: امنیت - موضوع: امنیت - موضوع: امنیت - موضوع: امنیت - موضوع: امنیت

<https://www.shabakeh-mag.com/security/5186>:موضوع: امنیت