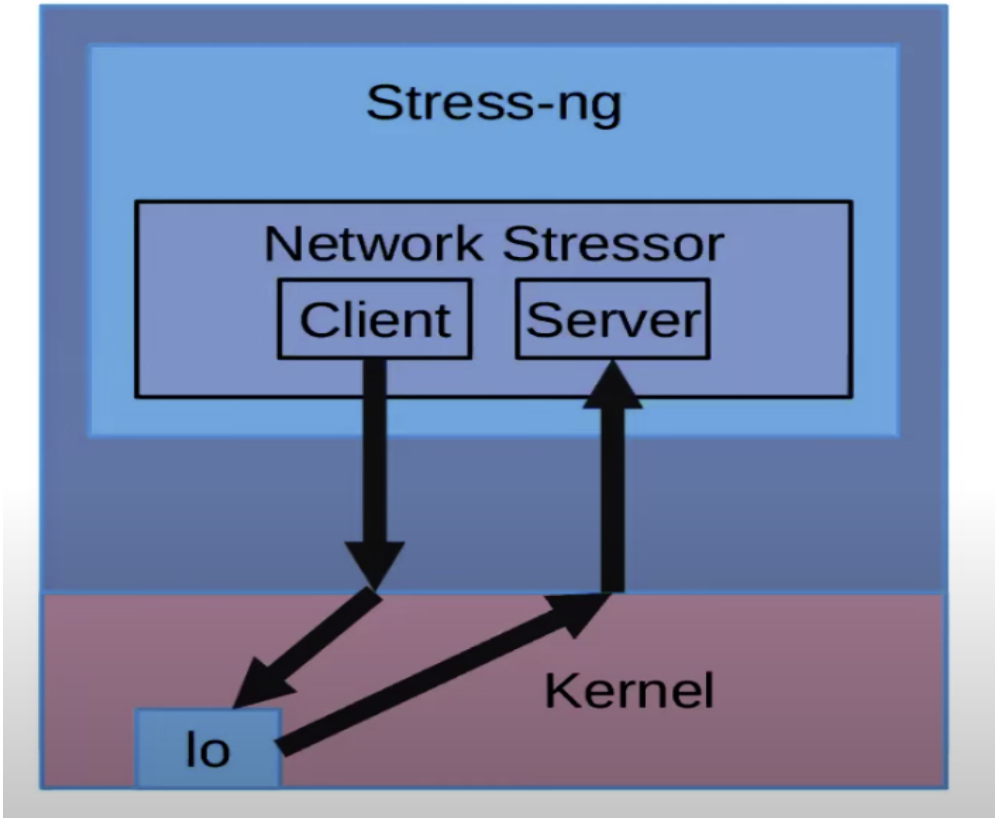
Introduction

This project includes what is side-channel attack and how Linux detects this attack with some measures. I am going to perform this eventually. The Linux Kernel is a core component of the Linux operating system, which manages memory allocation, processes, system resources and system calls.

The main goal of the side-channel attack is to gather information indirectly from systems or cryptographic algorithms instead of the algorithms' weaknesses [1].

Some attacks can be achieved by the side-channel attack, such as Timing Attack, Electromagnetic (EM) attack, Simple power analysis (SPA), Differential power analysis (DPA) and Template attack [2].

One of the tools we can use for performing a Side-Channel Attack is "**stress-ng"** [3], the installation is ***here*****,** and more detailed information is in this ***video*****.**



Objective

The cache-timing attack is one of the Side-Channel attacks used to exploit the system vulnerabilities with various inputs. Consequently, the attacker can fill up the cache for intended behaviours. Some commands are used to test CPU and Memory [5].

1. **Analyzing CPU cache with "Stress-ng":**

The below Figure 1 and Figure 2 are from the video.

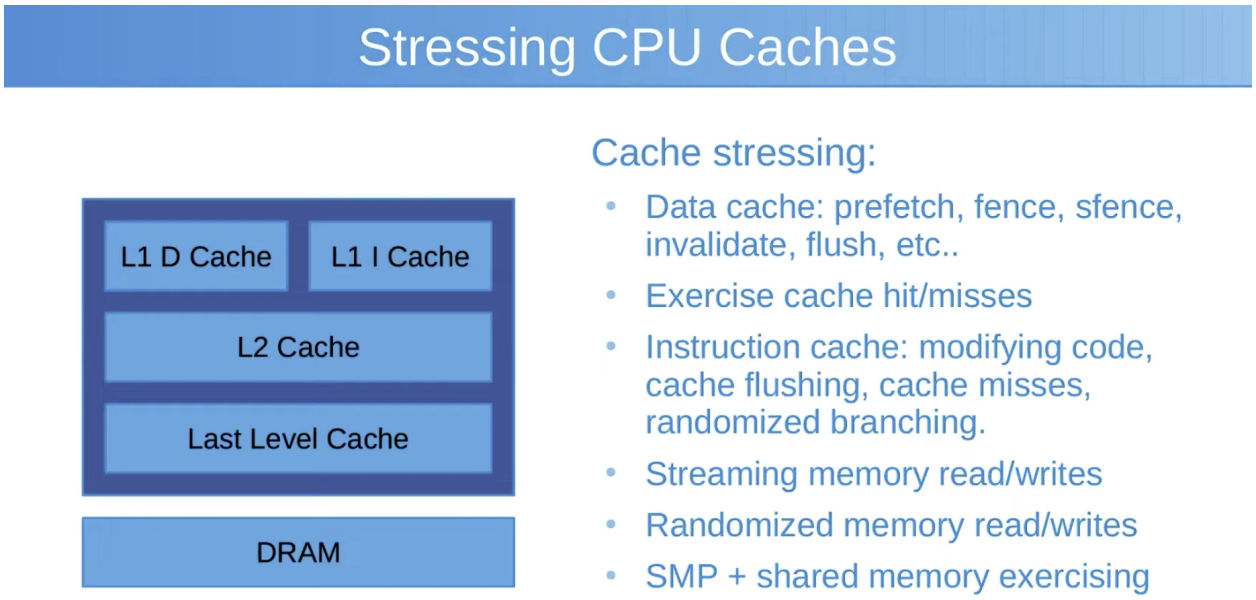


Figure 1.

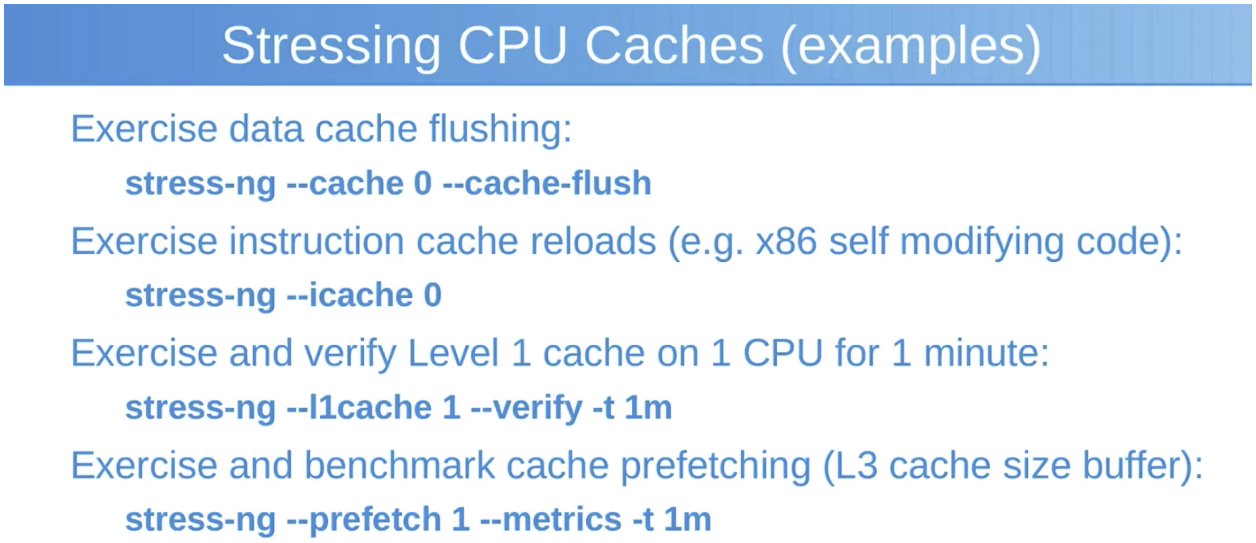


Figure 2.

The result shows that the CPU time will increase if I use "**stress-ng**" to flush the system's cache.

2. **Analyzing Kernel with "Stress-ng":**

Figure 3, and Figure 4 are from the video.

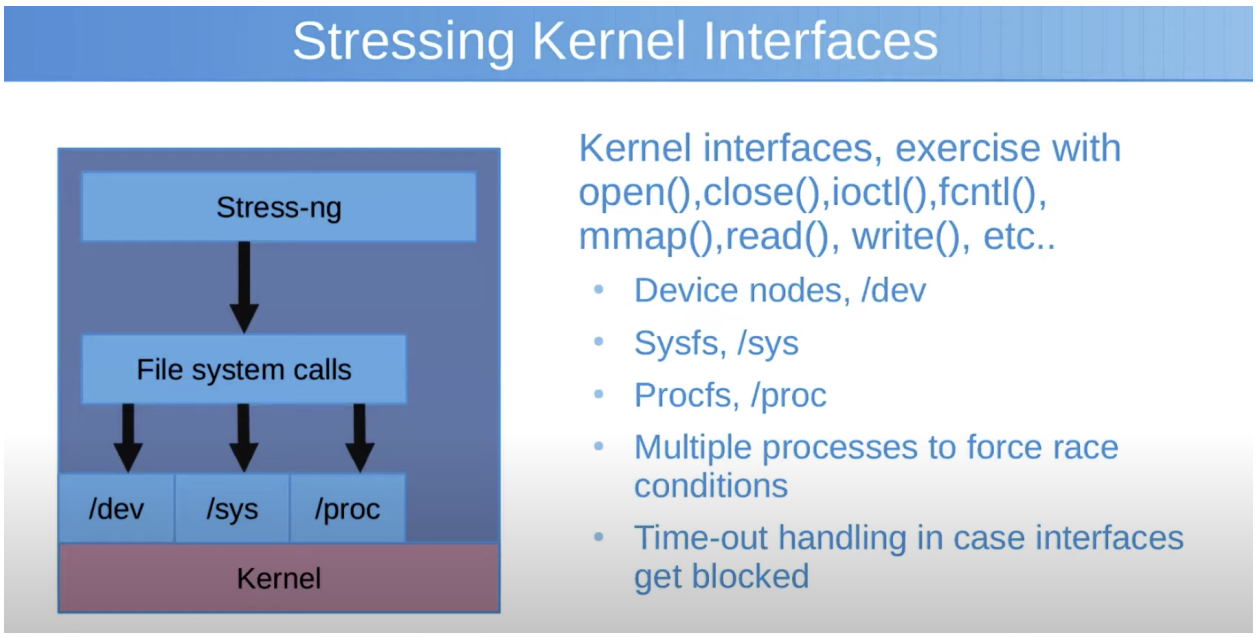


Figure 3.

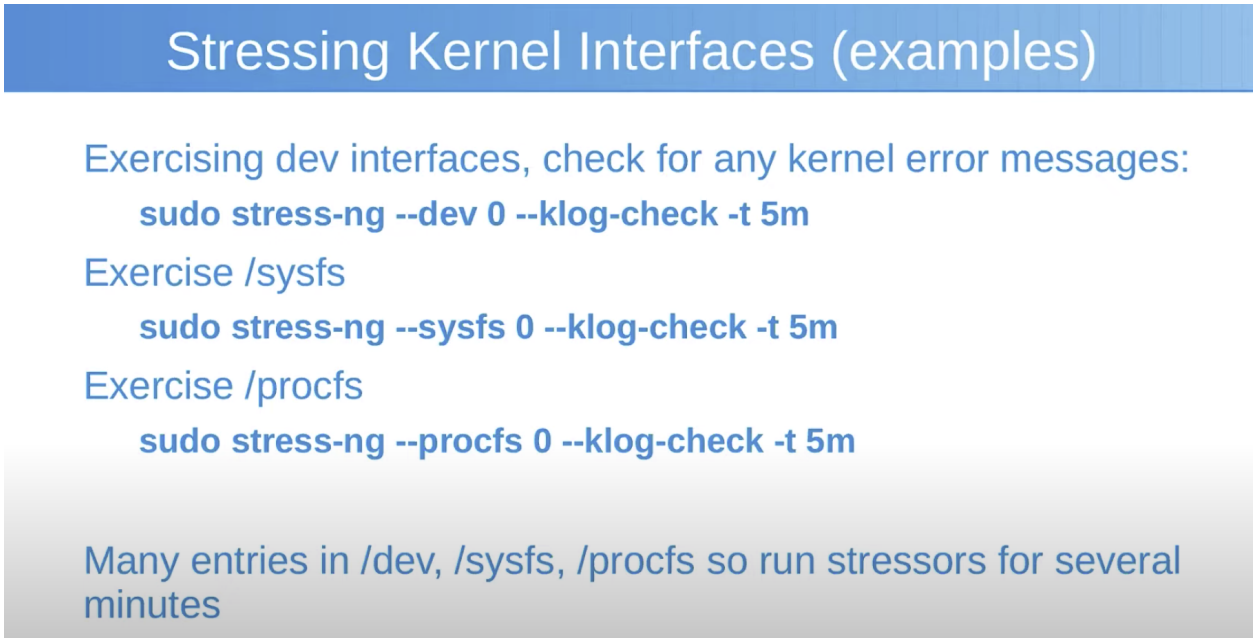


Figure 4.

Activity Questions:

1. What is the Side-Channel Attack?
2. BrieflyxExplain the relation between Side-channel Attacks with the "**stress-ng**" stress testing tool.
3. What are the countermeasures for Side-Channel Attacks (SCA)?

   Explain one of them.

Reference

1. J. Lake, “What is a side channel attack? (with examples),” *Comparitech*, 18-May-2021. [Online]. Available: https://www.comparitech.com/blog/information-security/side-channel-attack/. [Accessed: 11-Nov-2022].

2. R. Press, “Side-channel attacks explained: Everything you need to know,” *Rambus*, 10-Nov-2021. [Online]. Available: https://www.rambus.com/blogs/side-channel-attacks/#how. [Accessed: 12-Nov-2022].

3. “Product documentation for red hat enterprise linux 8,” *Red Hat Customer Portal*. [Online]. Available: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8. [Accessed: 16-Nov-2022].

4. “Stress test CPU and memory (VM) on a linux / unix with stress-ng.” [Online]. Available: https://www.cyberciti.biz/faq/stress-test-linux-unix-server-with-stress-ng/. [Accessed: 17-Nov-2022].