**AULA 2(17-11): ASPECTOS QUE DIFERENCIAM O SISTEMA OPERACIONAL DE DEMAIS SOFTWARES E MECÂNICOS PARA ACESSO PRIVILEGIADO A CPU**

A aula foi baseada no vídeo "*How a Single Bit Inside Your Processor Shields Your Operating System's Integrity*" do canal Core Dumped(https://youtu.be/H4SDPLiUnv4?si=sJ34VGMMSAYz6tdQ). Após a exibição do vídeo, a turma foi dividida em grupos e cada grupo discutiu tópicos explorados pelo conteúdo do vídeo. Dentre os quais estão:

- **Papel do Bit de modo:** basicamente, o bit de modo é responsável por sinalizar se o processo(ou software) em questão está trabalhando no modo usuário, isto é, sem acesso às instruções privilegiadas da CPU, ou em modo kernel, onde o processo tem acesso às tais instruções privilegiadas. Esse bit funciona como uma barreira de proteção: enquanto o processo estiver no modo usuário, qualquer tentativa de acessar instruções privilegiadas é barrada pelo automaticamente pelo hardware. Por fim, o valor indica modo Kernel e o valor 0 indica modo usuário.

- **Acesso às instruções privilegiadas:** certas operações, como o acesso à abertura, leitura e fechamento de arquivos, só podem ser realizadas no modo Kernel. Caso um software que esteja operando no modo usuário necessite de alguma dessas "operações" especiais, o mecanismo adotado é o seguinte: há uma instrução na linha de código desse programa que realiza uma interrupção, devolvendo o "controle" para o sistema operacional, que realiza a operação solicitada em modo Kernel. Após isso, o processo é retomado em modo usuário.

- **Troca de modo e chamadas de sistema:** o processo pelo qual é realizada a alternância entre o modo de usuário e o modo Kernel recebe o nome de *Chamada de sistema(ou syscalls)*. Essas chamadas de sistema são interrupções no processo que fazem o processador alternar temporariamente entre o modo Kernel e o modo usuário. Esse fluxo destaca como hardware e software cooperam para permitir que programas realizem tarefas avançadas sem comprometer a segurança e integridade do sistema.

- **Drivers e sua relação com o modo kernel:** Drivers são módulos de software responsáveis por permitir que o sistema operacional se comunique com dispositivos físicos, como placas de vídeo, controladores USB, discos rígidos, entre outros. Por precisarem acessar o hardware diretamente, os drivers operam em modo kernel, o que lhes dá privilégios muito elevados. Isso significa que qualquer erro, falha de implementação ou vulnerabilidade dentro de um driver pode comprometer a integridade do sistema como um todo. Desse modo, drivers são um dos elementos mais sensíveis do sistema, já que executam código privilegiado. Assim, o isolamento entre modo usuário e kernel ajuda a reduzir os danos causados por falhas, evitando que problemas em um driver "derrubem" completamente o sistema.

- **Importância do isolamento entre processos e kernel:** o isolamento entre o sistema operacional e as demais aplicações são uma das bases da segurança e integridade de um sistema, evitando falhas como loops infinitos, acessos indevidos e corrupção de memória.

## CONCLUSÕES

A aula reforçou como conceitos fundamentais de segurança em sistemas operacionais dependem diretamente do suporte do hardware. A existência de um simples bit no processador, responsável por diferenciar execução privilegiada e não privilegiada, garante que o sistema operacional mantenha seu controle e integridade. O mecanismo de mudança controlada entre os modos, somado às exceções e ao isolamento de memória, forma a base de um ambiente seguro, evitando que processos comprometam o funcionamento do sistema como um todo. Compreender como o hardware impõe limites ao software é essencial para o estudo de sistemas operacionais, especialmente no que diz respeito à segurança, estabilidade e design de arquiteturas modernas.

Aluno: João Victor Oliveira
Matrícula: 20240008468