Análise e desenvolvimento de sistemas
1º PERÍODO
Prof: Thalles Canela.
Alunos:
Lais Laylla
Luiz Felipe
Danilo Ribeiro
Vitória.

Arquitetura Em segurança de computadores

Segurança em Processadores: Estudo sobre vulnerabilidades como Spectre e Meltdown.

—

1. O que é A Segurança em Arquitetura de Computadores?

Segurança de computadores ou cibersegurança é a proteção de sistemas de computador contra roubo ou danos ao hardware, software ou dados eletrônicos, bem como a interrupção ou desorientação dos serviços que fornecem.

Qual á Importância da Arquitetura de Segurança em um Processador?

A Arquitetura de Segurança em um processador é crucial para proteger dados e operações contra ameaças, garantindo a integridade e confidencialidade das informações. Ela permite a implementação de mecanismos de segurança, como criptografia e execução isolada, que ajudam a mitigar vulnerabilidades e ataques cibernéticos.

- ### Principais Importâncias da Arquitetura de Segurança em um Processador

Proteção de Dados Sensíveis: A arquitetura de segurança assegura que dados críticos, como informações pessoais e financeiras, sejam armazenados e processados de forma segura, evitando acessos não autorizados.

Criptografia de Hardware: A implementação de algoritmos de criptografia diretamente no processador aumenta a eficiência e a segurança, protegendo dados em trânsito e em repouso.

Detecção de Ameaças: Processadores com arquitetura de segurança avançada podem incluir recursos para detectar e responder a comportamentos anômalos, ajudando a prevenir ataques em tempo real.

Resiliência a Ataques: A arquitetura de segurança é projetada para resistir a uma variedade de ataques, incluindo injeções de código e ataques de negação de serviço, aumentando a robustez do sistema.

Aumento da Confiança do Usuário: Um processador com arquitetura de segurança sólida contribui para a confiança do usuário em sistemas e dispositivos, essencial em um ambiente digital cada vez mais ameaçado.

Meltdown e Spectre: as falhas que afetam quase todos os processadores do mundo.

Meltdown e Spectre são vulnerabilidades de segurança que afetam processadores modernos, permitindo que atacantes acessem dados sensíveis. Meltdown é específico de processadores

Intel, enquanto Spectre afeta uma gama mais ampla, incluindo chips da AMD e ARM, explorando falhas na execução especulativa e no gerenciamento de memória.

O que é Meltdown?

O Meltdown consiste em quebrar um mecanismo de segurança dos processadores da Intel que previne aplicativos de acessarem a memória reservada ao kernel do sistema operacional. Ele se chama assim porque "derrete" (melt, em inglês) a barreira de defesa dos chips.

- A falha foi testada em processadores da Intel lançados desde 2011, mas deve atingir todos os chips fabricados pela empresa desde 1995 (com exceção dos Intel Itanium, com arquitetura diferente; e dos Intel Atom produzidos antes de 2013). O Meltdown funciona em desktops, laptops e servidores.

O que é Spectre?

O Spectre é uma falha mais difícil de corrigir, porque, para ser totalmente resolvida, exigiria que os chips fossem reprojetados. Sim: há uma falha de design em quase todos os processadores modernos do mercado. No entanto, as empresas já trabalham para mitigar o problema por software.

- Ambas têm implicações significativas para a segurança cibernética, exigindo que usuários e organizações implementem medidas de proteção adequadas.