Análise e desenvolvimento de sistemas
1º PERÍODO
Prof: Thalles Canela.

Arquitetura em segurança de Computadores

Segurança em Processadores: Estudo sobre Meltdown e Spectre

1.1 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.

1.2 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.

1.3. Principais Importâncias da Arquitetura de Segurança em um Processador

1.4. 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.

1.5. 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.

1.6. 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.

1.7. 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.

1.8. 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.

2.1. Vulnerabilidades Arquiteturais Famosas

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.

2.2. Ataques baseados em Cache
Flush+Reload, Prime+Probe: Explorando a latência de acesso à memória cache para inferir dados secretos.

Side-channel attacks: Usam efeitos colaterais da execução, como tempo de resposta, para acessar dados.

2.3. Falhas adicionais Foreshadow (L1TF): Vazamento de memória através de falhas na L1 cache.

ZombieLoad, Fallout, RIDL: Variantes que afetam arquiteturas x86.

3. Medidas de Segurança Arquitetural

3.1. Isolamento de Memória

Projetos modernos implementam isolamento físico e virtual para evitar acesso cruzado entre processos.

3.2. Execução Segura (Intel SGX, AMD SEV)

Técnicas que permitem criar áreas de memória seguras chamadas “enclaves”, onde nem o sistema operacional consegue acessar os dados.

3.3. Criptografia baseada em Hardware

Alguns chips modernos possuem motores de criptografia dedicados, evitando que dados sensíveis sejam manipulados em software.

3.4. Boot Seguro (Secure Boot)

Valida a integridade do sistema durante a inicialização, impedindo que softwares não autorizados sejam executados.

4. Comparação entre Arquiteturas

4.1. Intel x ARM

Intel: Mais suscetível a falhas de execução especulativa devido à complexidade das microarquiteturas CISC.

ARM: Adota arquiteturas RISC, mais simples e com menor histórico de falhas desse tipo, embora não totalmente imune.

4.2. RISC-V

Arquitetura aberta que permite que empresas adaptem o hardware com foco em segurança desde o início do projeto.

6. Impactos Reais

Ataques baseados em arquitetura têm impactos que vão desde o roubo de senhas até espionagem em larga escala. Como muitas dessas falhas não podem ser corrigidas apenas por software, elas pressionam a indústria a repensar os fundamentos de segurança do hardware