Falhas Spectre e Meltdown

As falhas Meltdown e Spectre - duas vulnerabilidades relacionadas que permitem uma ampla variedade de divulgação de informações de cada processador mainstream, com falhas particularmente severas para a Intel e alguns chips ARM - foram originalmente reveladas em particular para empresas de chips, desenvolvedores de sistemas operacionais e provedores de computação em nuvem.

Os processadores modernos executam a execução especulativa. Para maximizar o desempenho, eles tentam executar instruções antes mesmo de ter certeza de que essas instruções precisam ser executadas. Por exemplo, os processadores tentam adivinhar de que maneira uma ramificação será tomada e executaram instruções com base nessa suposição. Se o palpite estiver correto, ótimo; o processador consegue algum trabalho sem ter que esperar para ver se o ramo foi tirado ou não. Se o palpite estiver errado, os resultados são descartados e o processador continua executando o lado correto da ramificação. Embora essa execução especulativa não altere nem um pouco o comportamento do programa, a pesquisa sobre Espectro e Fragmentação demonstra que isso perturba o estado do processador de maneiras detectáveis. Essa perturbação pode ser detectada medindo cuidadosamente quanto tempo leva para executar determinadas operações. Usando esses intervalos, é possível que um processo inferir propriedades de dados pertencentes a outro processo - ou até mesmo o kernel do sistema operacional ou o hipervisor da máquina virtual.

Esse vazamento de informações pode ser usado diretamente, por um JavaScript malicioso em um navegador que pode roubar senhas armazenadas no navegador. Ele também pode ser usado em conjunto com outras falhas de segurança para aumentar seu impacto. O vazamento de informações tende a minar as proteções, como o ASLR (randomização do layout do espaço de endereço), de modo que essas falhas podem permitir o uso efetivo de estouros de buffer .

O Meltdown, aplicável a praticamente todos os chips Intel fabricados há muitos anos, juntamente com determinados projetos ARM de alto desempenho, é o mais fácil de explorar e permite que qualquer programa de usuário leia vastos trechos de dados do kernel. A falha depende da maneira como os sistemas operacionais compartilham a memória entre os programas do usuário e o kernel, e a solução é pôr fim a esse compartilhamento.

O Specter, aplicável a chips da Intel, AMD e ARM, e provavelmente a todos os outros processadores no mercado que oferecem execução especulativa, também é mais sutil. Ele engloba um truque testando limites de matriz para ler memória em um único processo, que pode ser usado para atacar a integridade de máquinas virtuais e de áreas restritas e ataques de processo cruzado usando os preditores de ramificação do processador (o hardware que advinha qual lado de uma ramificação é tomadas e, portanto, controla a execução especulativa). Correções sistêmicas para alguns aspectos do Specter parecem ter sido desenvolvidas, mas a proteção contra toda a gama de correções exigirá modificação (ou pelo menos recompilação) de programas em risco.

FONTE:
https://arstechnica.com/gadgets/2018/01/meltdown-and-spectre-heres-what-intel-apple-microsoft-others-are-doing-about-it/