Aluno:Luis Henrique Matos Sales

Invasão processadores Intel

Com Spectre

O nome do Spectre está relacionado à causa do problema, que é a execução especulativa (speculative execution, em inglês). Para acelerar o desempenho dos softwares, os processadores modernos tentam adivinhar qual código será executado em seguida. Caso a previsão esteja errada, o resultado é simplesmente descartado; caso esteja certa, há uma economia de tempo.

O Spectre é uma falha mais difícil de corrigir, porque, para ser totalmente resolvida, exigiria que os chips fossem reprojetados. No entanto, a tecnologia também pode induzir um processador a executar uma operação “adivinhada” que não seria executada em condições normais. Isso permite que um aplicativo vaze uma informação confidencial para outro aplicativo, quebrando vários mecanismos de segurança de softwares.

Segundo pesquisadores da página oficial do Meltdown e do Spectre muito provavelmente todos são afetados, mas ainda não há relatos de que as brechas foram exploradas. Essas brechas atingem desktops,laptops, servidores, smartphones e qualquer outro dispositivo com alta capacidade de processamento.

Diferente de malware comum, os antivírus não detectam tão facilmente um aplicativo que se aproveite do Meltdown ou do Spectre. Além da exploração das vulnerabilidades não deixar nenhum rastro no sistema, o que torna difícil descobrir se uma pessoa já foi ou não atingido pelas brechas.

Fonte: https://tecnoblog.net/231300/meltdown-spectre-intel-amd-arm-falha-processadores/