Falha Spectre nos Processadores Intel

No inicio de 2018 ocorreu uma grande falha de segurança nos chips da Intel e esta falha permitia que um aplicativo comum tivesse acesso a áreas protegidas da memória do sistema operacional, expondo informações sensíveis. E há uma brecha também que acabou afetando os processadores da ARM e da AMD. O nome Spectre está relacionado à causa do problema, que é a execução especulativa que é usada 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 descartado se não há uma economia de tempo.

E isso foi feito com Meltdown que é um mecanismo que propõe fazer o que já diz o próprio nome, derreter a segurança. Isso foi feito quebrando um mecanismo de segurança dos processadores da Intel que prevenia que os dados de memoria reservada do kernel do sistema. E essa quebra de segurança faz com que um aplicativo vaze uma informação confidencial para outro aplicativo, quebrando vários mecanismos de segurança de softwares

O Spectre é uma falha mais difícil de corrigir, porque, para ser totalmente resolvida, exigiria que os chips fossem projetados novamente, pois, há uma falha de design. Mas as empresas estão trabalhando para resolver isso usando o próprio software para que ele cubra essa falha usando um patch que consiste em isolar completamente os processos de usuários e a memória do kernel, é possível que haja redução no desempenho entre 5 e 30%.