

# Bem vindo ao Cybergeddon - O "apocalipse dos processadores" é muito pior do que você imagina.

[Alberto J Azevedo](#) Jan 5, 2018

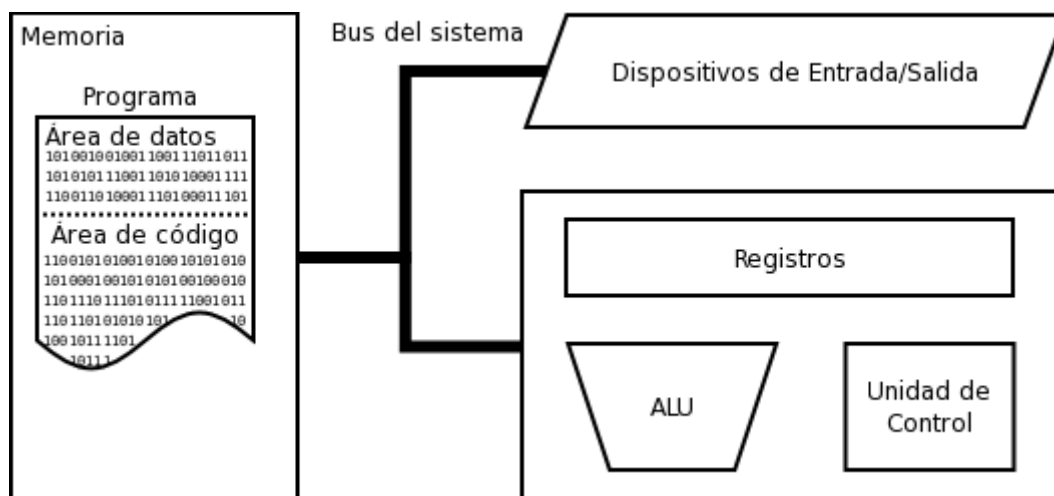


O mundo entrou em pânico essa semana e a razão é simples: vieram a público duas vulnerabilidades extremamente graves que afetam virtualmente (praticamente) todos os processadores em uso no mundo. Logo que elas vieram a público vieram também duas outras informações no mínimo "desconcertantes". A primeira de que a falha já havia sido comunicada aos fabricantes nada menos do que SEIS meses atrás e a segunda de que Brian Krzanich, CEO da Intel, malandramente vendeu nada menos que [METADE de suas ações](#) ficando com o mínimo que ele legalmente podia ficar quando soube das falhas há alguns meses atrás. A razão para as fabricantes estarem sabendo disso a seis meses e não terem feito nada, e Brian Krzanich ter feito o que fez é simples: as falhas, e principalmente seus impactos e dificuldades no processo de correção, são muito mais graves do que você pode imaginar.

Mas vamos começar pelo começo. O ano era 1946 e um matemático húngaro de nome [John von Neumann](#) com sua equipe de pesquisadores no IAS (Princeton Institute for Advanced Studies), desenvolveu um novo modelo computacional, onde uma máquina digital podia armazenar seus programas no mesmo espaço de memória que os dados, podendo assim manipular tais programas. Isso resolvia uma série de limitações que o modelo fixo, adotado até então, possuía. Naquela época os computadores não eram tão programados, mas praticamente "desenhados". Sua função era estabelecida, eram concebidos os desenhos esquemáticos de como ele faria aquilo, isso era escrito, e pronto. Ou seja se você criasse um computador capaz de fazer bolo de chocolate, ele faria bolo de chocolate pro resto da vida. Caso você quisesse mudar isso, ou ensinar ele a fazer um novo tipo de cobertura, você teria um processo extremamente penoso, em que você seria preciso reprojetar a máquina como um todo, podendo levar semanas para criar um programa no ENIAC e voltar a trabalhar. O modelo de Von Neumann era revolucionário, mudava radicalmente a forma de como as coisas eram feitas e criava inúmeras novas possibilidades para a computação. Entenda, ele possibilita que a máquina agora trate as instruções recebidas, e essa a capacidade de tratar as instruções como os dados é o que faz montadores, compiladores e outras ferramentas de programação automatizada possíveis. Era sensacional.

Mas haviam problemas e críticas. A primeira e mais óbvia, mesmo à época era o gargalo. O canal de transmissão de dados entre a CPU e a memória leva ao que ficou conhecido como gargalo de von Neumann, a troca de dados limitada (taxa de transferência) entre a CPU e a memória em relação à quantidade de memória. Na maioria dos computadores modernos, a troca de dados entre o processador e a memória é muito menor do que a taxa com que o processador pode trabalhar. Isso limita seriamente a velocidade eficaz de processamento, principalmente quando o processador é exigido para realizar o processamento de grandes quantidades de dados. A CPU é constantemente forçada a esperar por dados que precisam ser transferidos para, ou a partir

da, memória. Como a velocidade da CPU e o tamanho da memória têm aumentado muito mais rapidamente que a taxa de transferência entre eles, o gargalo se tornou mais um problema, um problema cuja gravidade aumenta com cada geração de CPU.



Além disso, uma vez que os programas estão sendo armazenados no mesmo espaço que os dados, alterar o programa pode ser extremamente prejudicial. Quer por acidente ou uma falha no design, um programa com defeito pode alterar outros programas ou, até mesmo, o sistema operacional. Vários matemáticos, entre eles [Alan Turing](#), se opunham ao modelo de Von Neumann, apontando as falhas matemáticas no processo e escrevendo artigos propondo outros modelos, mas o envolvimento de Neumann no projeto Manhattan e projeto ENIAC fez com que sua concepção para o EDVAC alcançasse maior circulação. O resto é história.

Vapt, voltamos pra 2017! Ao longo dos anos, essa limitação na arquitetura já causou inúmeros problemas. [Praticamente todas as vulnerabilidades de memória que tivemos nos últimos anos tiram proveito dessa escolha de design](#), que hoje mostrou seu verdadeiro potencial destrutivo. Mas entenda, caro leitor, eu não estou culpando Von Neumann pela falha de hoje, isso seria o equivalente a culpar o McDonald's por essa sua pança gorda. Os culpados são as centenas de engenheiros que vieram posteriormente e não tiveram peito para fazer o que vão ter que fazer agora: um completo redesign e reestruturação da arquitetura, face aos novos desafios e realidade da computação hoje em dia. Isso porque (spoiler alert) a vulnerabilidade que foi nomeada spectre, a princípio, simplesmente não pode ser corrigida com um patch!!! Ela vai exigir um redesign dos processadores. Você está entendendo, caro leitor? Virtualmente todos, eu repito, TODOS os processadores em uso no mundo hoje precisarão ser TROCADOS!!!! Está entendendo porque o caldo é muito mais embaixo? Esta entendendo o porquê de os fabricantes não terem feito nada até agora, mesmo tendo tido seis meses para fazer? Bom o Brian fez: vendeu todas as ações que ele podia, porque ele sabia, há meses atrás, o que o mundo ficou sabendo agora. Veja, não existe nem capacidade de produção para realizar as trocas que precisam ser feitas. O assunto é muito sério.



Bom, mas primeiro vamos explorar e explicar rapidamente os problemas. Meses atrás, alguns pesquisadores de segurança independentes e outros dentro do projeto Google Project Zero descobriram duas vulnerabilidades nos processadores que foram chamadas de Meltdown e Spectre. Elas permitem a atacantes maliciosos roubar / acessar todo o conteúdo de memória de computadores, celulares e servidores. A primeira, Meltdown, está limitada a processadores Intel e quebra o isolamento existente entre as aplicações do usuário e sistema operacional. Você pode achar mais informações [aqui](#), além de ver uma PoC [aqui](#) e [aqui](#). Para essa vulnerabilidade existem alguns patches de correção que já estão sendo disponibilizados, porém elas causarão uma redução na capacidade de processamento que pode variar entre 5% e 30%. Ao passo que será um certo incomodo para o usuário final perder cerca de 30% da capacidade de processamento de sua estação. Você, caro leitor, faz alguma ideia do impacto financeiro que isso representa para uma Amazon por exemplo? Amazon, Microsoft, Google, entre outras grandes players do mercado de cloud, terão prejuízos astronômicos com as falhas e a lentidão que as correções venham a eventualmente causar, isso porque, de uma hora pra outra, seu parque computacional, simplesmente não acomodará mais o uso que vem sendo feito dele. Note


que, enquanto em seu computador, um atacante pode roubar informações suas, em um servidor virtualizado ele pode roubar informações de todas as pessoas/empresas que estão acomodadas naquele virtualizador. Estamos falando de senhas, dados, chaves de criptografia, qualquer coisa.

Agora veja que o patch de correção embora exista para o caso do Meltdown, precisa ser aplicado por cada administrador de sistemas do planeta em seus equipamentos. Lembram do WannaCry? Aquela vulnerabilidade foi descoberta e já havia uma correção disponível há meses. Está entendendo o problema? Pior o Meltdown pode ser explorado por qualquer script-kiddie com acesso a um computador e dois neurônios funcionais.

Já, por sorte, a exploração da Spectre é mais complexa de ser realizada, e digo sorte, porque como foi dito, na teoria, simplesmente não existe correção possível para a vulnerabilidade. Será necessário um redesign completo dos processadores e Intel, AMD e ARM terão que fazer um recall completo de todos os processadores já fabricados, na prática, os problemas serão resolvidos somente no próximo ciclo de vida dos hardwares, ou seja, sentiremos os efeitos pela próxima década. Basicamente o que ocorreu é que na ânsia e guerra pela performance e capacidade, as fabricantes se tornaram desleixadas com a segurança. Não é de hoje que isso é questionado por pesquisadores de segurança no mundo inteiro. Tanto que muitos equipamentos de missão crítica são equipados com os chamados processadores seguros. Processadores feitos por empresas como a [Kryptus](#), empresa estratégica de defesa nacional pertencente aos amigos Gallo e Henrique e o seu Secure Crypto-processor (SCuP) ou os [Secure Processors](#) fabricados pela Broadcom por exemplo.

A [Spectre](#) foi chamada dessa maneira pois explora o que chamamos de capacidade de execução especulativa dos processadores, pois basicamente processadores modernos usam técnicas como branch prediction e speculative execution para maximizar a performance. Lembram do gargalo do Von Neumann? Essas são algumas das técnicas adotadas pra tentar mitigar esse problema. Na prática, se o destino dos dados de um branch dependem de dados que ainda estão sendo lidos na memória, a CPU vai tentar "especular" (adivinhar/prever) qual é esse destino e executar na frente. Quando os dados de fato chegarem, ela irá ou confirmar ou descartar essa previsão. O ataque consiste em abusar dessa capacidade especulativa dos processadores, e induzir a vítima a realizar operações que não iriam ocorrer normalmente, o que leva ao vazamento de informações via side-channel. Você pode ver um exemplo de implementação [aqui](#). Embora seja possível mitigar os efeitos da spectre via microcódigo, a solução só vai ocorrer através de um redesign dos processadores, o que absolutamente não ocorrerá de forma rápida. O problema é que na guerra entre segurança e velocidade foram sendo feitas concessões em nome da performance. A conta está chegando agora.

 Software Engineering Institute | Carnegie Mellon University

 Homeland Security  
Sponsored by the DHS Office of Cybersecurity and Communications

**Vulnerability Notes Database**  
Advisory and mitigation information about software vulnerabilities

[DATABASE HOME](#) [SEARCH](#) [REPORT A VULNERABILITY](#) [HELP](#)

### Vulnerability Note VU#584653

#### CPU hardware vulnerable to side-channel attacks

Original Release date: 03 Jan 2018 | Last revised: 03 Jan 2018

[Print](#) [Tweet](#) [Send](#) [Share](#)

#### Overview

CPU hardware implementations are vulnerable to side-channel attacks. These vulnerabilities are referred to as Meltdown and Spectre.


#### Description

CPU hardware implementations are vulnerable to side-channel attacks referred to as Meltdown and Spectre (also KAISER and KPTI). These attacks are described in detail by Google Project Zero and the Institute of Applied Information Processing and Communications (IAIK) at Graz University of Technology (TU Graz).

#### Impact

An attacker able to execute code with user privileges can achieve various impacts, such as reading otherwise protected kernel memory and bypassing KASLR.

**Solution**  
Replace CPU hardware



The underlying vulnerability is primarily caused by CPU architecture design choices. Fully removing the vulnerability requires replacing vulnerable CPU hardware.

**Quick Search**


Go

Advanced Search »


**View Notes By**

- Date Published
- Date Public
- Date Updated
- CVSS Score

**Report a Vulnerability**

 Please use the Vulnerability Reporting Form to report a vulnerability. Alternatively, you can send us email. Be sure to read our vulnerability disclosure policy.

**Connect with Us**

 Subscribe to our feed

De qualquer maneira, esse incidente pode trazer resultados positivos. A primeira, deve ser uma profunda reflexão por parte do mercado do perigo existente em se ficar dependente de tão poucos players de mercado. Veja, o mercado de processadores está literalmente nas mãos de três empresas. Somos totalmente dependentes delas, de suas vontades e de suas decisões. Outro benefício será uma maior atenção e importância a ser dada às questões de segurança. O dilema Segurança x Velocidade já é antigo. Se você tem um baú, colocar um cadeado nele o deixará mais seguro, mas vai levar mais tempo para abri-lo e fechá-lo todas as vezes que você precisar fazer isso durante o dia. E nessa discussão até hoje a performance tem sempre vencido a segurança. Bom, pode ser que isso mude agora. Outra vantagem vai ser o fato de que tecnologias como [Field-Programmable Gate Array \(FPGA\)](#) e [Complex Programmable Logic Device \(CPLD\)](#) devem ganhar mais evidência agora, uma vez que apresentam muito mais recursos e possibilidades de personalização do que as tecnologias em uso hoje.

Resumindo, a solução não vai ser simples a [Intel está claramente tentando acalmar os ânimos](#), mas a questão é muito séria. Como foi dito, a Meltdown pode ser explorada até pela minha filha de cinco anos; já a Spectre pode ser explorada por pessoal mais qualificado, por agentes do estado, ou patrocinados por ele. O que levanta a pergunta: Há quanto tempo você acha que a NSA, por exemplo, já não vem explorando essas falhas secretamente? Agora pense... Ambas as vulnerabilidades podem ser exploradas até mesmo [via browser!](#) A correção de uma delas pode vir a implicar na perda de até 30% de performance e a outra não tem correção definitiva possível (a não ser a troca do processador) o que implica em um recall completo de todos os processadores já fabricados em uso e sua substituição por novos com um redesign que ainda não existe. Mesmo que as fabricantes estivessem dispostas a ir à falência para tentar fazer isso em tempo recorde, a tecnologia ainda não existe. O projeto completo de um novo processador pode levar anos, e nem temos a capacidade de produção necessária para atender a um volume dessa magnitude. Consegue entender agora porque elas não fizeram nada de muito concreto nesses seis meses que sabem das falhas? Consegue entender as implicações disso tudo?

Bem vindo ao Cybergeddon!