# Side-Channel Attack

Leonardo Costa Santos - 10783142
Lucas Paiolla Forastiere - 11221911
Julia Leite - 11221797

1 de dezembro de 2020

# 1 Introdução

Side-Channel Attacks, que do inglês significa, Ataque por Canal Lateral são jeitos explorar vunerabilidades físicas de componentes eletrônicos, como a CPU de um computador.

O nome vem do fato deles não atacarem "pela porta da frente", mas sim algum "rastro"físico que um componente deixa ao fazer determinadas ações.

Um SCA não necessariamente tem a ver com componentes eletrônicos, pois podemos, por exemplo, descifrar uma senha de alguém captando os sons do teclado. Em geral, o SCA ataca um ponto fraco de um componente que não tem nada a ver com o seu funcionamento em si (como no exemplo do teclado, o teclado teoricamente não tem a responsabilidade de deixar os barulhos de cada tecla iguaizinhos). Daí então o nome *canal lateral*.

Os dois principais SCA, que tornaram o "ramo" famoso foram o *Meltdown* e o *Spectre*, descobertos por independentemente por uma série de pesquisadores, mas destacando-se o grupo Project Zero da Google [6].

Entretanto, existem muitas classes de SCA, como ataques ao cache (que é o caso dos dois exemplos citados), ataques que monitoram a energia consumida pelo computador, ataques que monitoram o eletromagnetismo eminido, ataques que monitoram o som emitido (como o exemplo do teclado), ataques que recuperam dados excluidos do disco entre muitos outros.

# 2 História

Um dos mais notórios ataques análogo ao que hoje conhecemos como ataque por canais laterais, foi chamado, pela *National Security Agency* (NSA) de Tempest[7] [10], e ocorreu em 1943, quando pesquisadores do *Bell Lab* descobriram que, utilizando um osciloscópio, era possível recuperar 75% do texto da mensagem emitita por um *teletype machine* há 80 pés (aproximadamente 24.3m) de distância.

Entretanto, o termo *Side Channel Cryptanalysis* sugiu apenas em 1998, em um artigo [5] onde uma equipe formada por criptógrafos da Counterpane Systems e pesquisadores da *Universy of California at Berkley* descreveu como ataques por canais laterais podem ser usados para quebrar sistemas de criptografia.

Em 2014, pesquisadores da *Tel Aviv University* [3] desenvolveram um dispositivo capaz de descobrir senhas criptografadas de laptop's próximos motitorando sua emissão elétrica. Além disso, em agosto do mesmo ano, esse grupo de pesquisadores publicou um artigo mostrando que o padrão sons emitidos por um computador durante o processo de descriptografia, detectável por um microfone, varia de acordo com a chave RSA utilizada, apesar disso, não ficou claro como extrair os bits da chave RSA.[4]

Desde 2018, o termo *side channel attack* se popularizou graças à descoberta de vunerabilidades presentes na maioria dos processadores Intel fabricados nas últimas duas décadas, exploradas por SCA como Meltdown, Spectre, entre outros.

# 3 Classificações de Side-Channel Attacks

## 3.1 Classificação por (?)

## 3.2 Classificação por grau da invasão

# 4 Exemplos de Side-Channel Attacks

## 4.1 Meltdown

Teste citando [6]

## 4.2 Spectre

## 4.3 CacheOut

## 4.4 SGAxe

## 4.5 ZombieLoad

Em 14 de maio de 2019 um grupo formado por pesquisadores de diversas universidades, dentre elas a austríaca Graz University of Technology e a belga Catholic University of Leuven, e por equipes das empresas de segurança Oracle, Cyberus, entre outras, juntamente com a Intel, reportou uma novo tipo de SCA, nomeado ZombieLoad [8], que explora vulnerabilidades presentes na maioria dos processadores Intel fabricados após 2011.[1]

O ZombieLoad, assim com o Spectre, Meltdown, Foreshadow, entre outros, pertence à classe dos *transient-execution attacks* [2], ataques que exploram vulnerabilidades resultantes de técnicas utilizadas para melhorar a performance do computador, como a execução fora de ordem e a execução especulativa. A primeira é um paradigma que permite que a CPU, ao invés de executar as microoperações de um conjunto de instruções sequencialmente, execute-as em paralelo, mesmo que a microoperação anterior não tenha sido finalizada, e as reorganize depois, decidindo aproveitar ou descartar os resultados. Já a segunda consiste na CPU executar instruções especulativamente, ou seja, antes delas aparecerem na lista de instruções, utilizando análise do fluxo de dados e predicção de desvio, assim como na técnica anterior, os resultados das instruções executadas especulativamente podem ser aproveitados ou descartados.

Nesse caso, chamamos essa instrução executada fora de ordem ou especulativamente, cujo resultado foi descartado de *transient instruction*. Os efeitos da *transient execution* são descartados, contudo, utilizando canais laterais como o *CPU cache subsystem*, é possível extrair dados de outros processos carregados no mesmo core da CPU, como senhas, tokens, histórico de navegação do browser, entre outros.

A Intel liberou correções em microcódigo para os processadores vulneráveis e a 8ª e 9ª geração de processadores possuem correção em hardware. Contudo, essas mitigações reduzem a velocidade do computador em 3% e a potência em 9%. Os pesquisadores, no entanto, afirmam que essas medidas são insuficientes para evitar que um computador esteja vulnerável a esse ataque e que a solução mais segura seria desabilitar o *hyperthreading*. [9]

## 4.6 Foreshadow

# 5 Há jeito de se previmir?

## 6 Há como saber se estou sofrendo um SCA?

No. =(=

# 7 Conclusão

# Referências


[1] Em: URL: https://www.wired.com/story/intel-mds-attack-speculative-execution-buffer.

[2] Claudio Canella et al. *A Systematic Evaluation of Transient Execution Attacks and Defenses*. 2019. arXiv: 1811.05441 [cs.CR]. URL: https://arxiv.org/pdf/1811.05441.pdf.

[3] Daniel Genkin et al. "Physical Side-Channel Key-Extraction Attacks on PCs". Em: 2015. URL: https://www.tau.ac.il/~tromer/radioexp/.

[4] Daniel Genkin et al. "RSA Key Extration via Low-Bandwidth Acoustic Cryptanalysis". Em: 2014. URL: https://www.tau.ac.il/~tromer/acoustic/.

[5] David Wagner John Kelsey Bruce Schneier e Chris Hall. "Side Channel Cryptanalysis of Product Ciphers". Em: (1998). URL: https://www.schneier.com/wp-content/uploads/2016/02/paper-side-channel.pdf.

[6] Moritz Lipp et al. "Meltdown: Reading Kernel Memory from User Space". Em: *27th USENIX Security Symposium (USENIX Security 18)*. 2018.

[7] NSA. "TEMPEST: A Signal Problem". Em: 2007. URL: https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/cryptologic-spectrum/tempest.pdf.

[8] Michael Schwarz et al. "ZombieLoad: Cross-Privilege-Boundary Data Sampling". Em: *CCS*. 2019.

[9] Cyberus Technology. "ZombieLoad: Cross Privilege-Boundary Data Leakage". Em: 2019. URL: https://www.cyberus-technology.de/posts/2019-05-14-zombieload.html.

[10] "What is a Side Channel Attack". Em: URL: https://www.wired.com/story/what-is-side-channel-attack/.