Side-Channel Attack

Leonardo Costa Santos - 10783142

Lucas Paiolla Forastiere - 11221911

Julia Leite - 11221797

18 de novembro 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 [1].

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

Primeira pessoa a usar o termo (Side Channel Cryptanalysis of Product Ciphers) Primeiro ataque descoberto (TEMPEST 1942) Popularização do termo Mais descobertas de ataques

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 [1]

4.2 Spectre

4.3 CacheOut

4.4 SGAxe

4.5 ZombieLoad

4.6 Foreshadow

5 Há jeito de se previmir?

6 Há como saber se estou sofrendo um SCA?

No. =(=

7 Conclusão

Referências

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