Side-channel Attacks

Tiago Rodeghiero

Sobre / Tiago Rodeghiero

Estudante de Segurança da Informação, 2017 - Atual

Atuação Profissional

Hacker Security, 2018 - Atual

Gtek - Soluções Tecnológicas, 2018 - Atual

O que são Side-channel Attacks?

O que são Side-channel Attacks?

São ataques que exploram as características físicas dos dispositivos buscando padrões de comportamento em determinadas ações para descobrir informações sobre um sistema.

Um Pouco de História

Ataques de canal lateral são divididos por períodos de estudo de acordo com o tipo de ataque realizado.

Ataques de indução a falha são estudados desde a década de 70.

Um Pouco de História

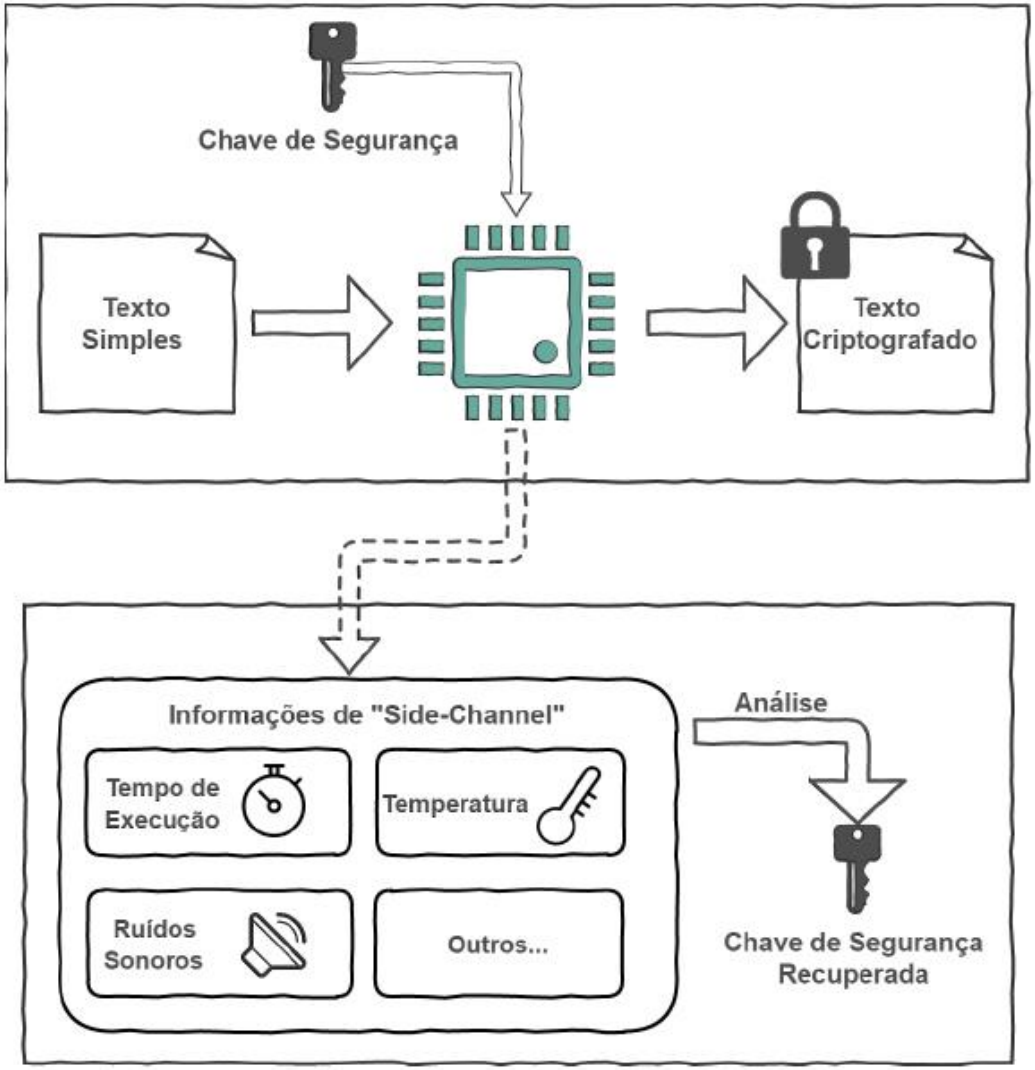
Anos 90.

Um dos primeiros artigos a chamar a atenção (teórica) para a ideia de usar ataques de temporização para quebrar sistemas criptográficos surgiu na década de 90.

Forneceu a base teórica, mas não foi considerada uma grande preocupação na época.

Paul C Kocher

Entendendo Um Ataque



SIDE CHANNEL

---------- attacks ----------

POWER ANALYSIS

O consumo de energia de um dispositivo pode revelar informações sobre quais operações estão sendo realizadas.

ACOUSTIC

Se beneficia da análise de sons para obter informações, pode ir desde os sons gerados por uma pessoa digitando no teclado até sons ocasionados por circuitos internos.

TIMING

Ataque que busca comprometer um dispositivo ou sistema através da análise de tempo entre suas operações.

OPTICAL

Analisa as emanações luminosas dos dispositivos para obter informações sigilosas.

ELECTROMAGNETIC

Movimentos de cargas elétricas são acompanhados por campos eletromagnéticos. As correntes que passam por um processador podem caracterizá-lo de acordo com sua assinatura espectral.

THERMAL IMAGING

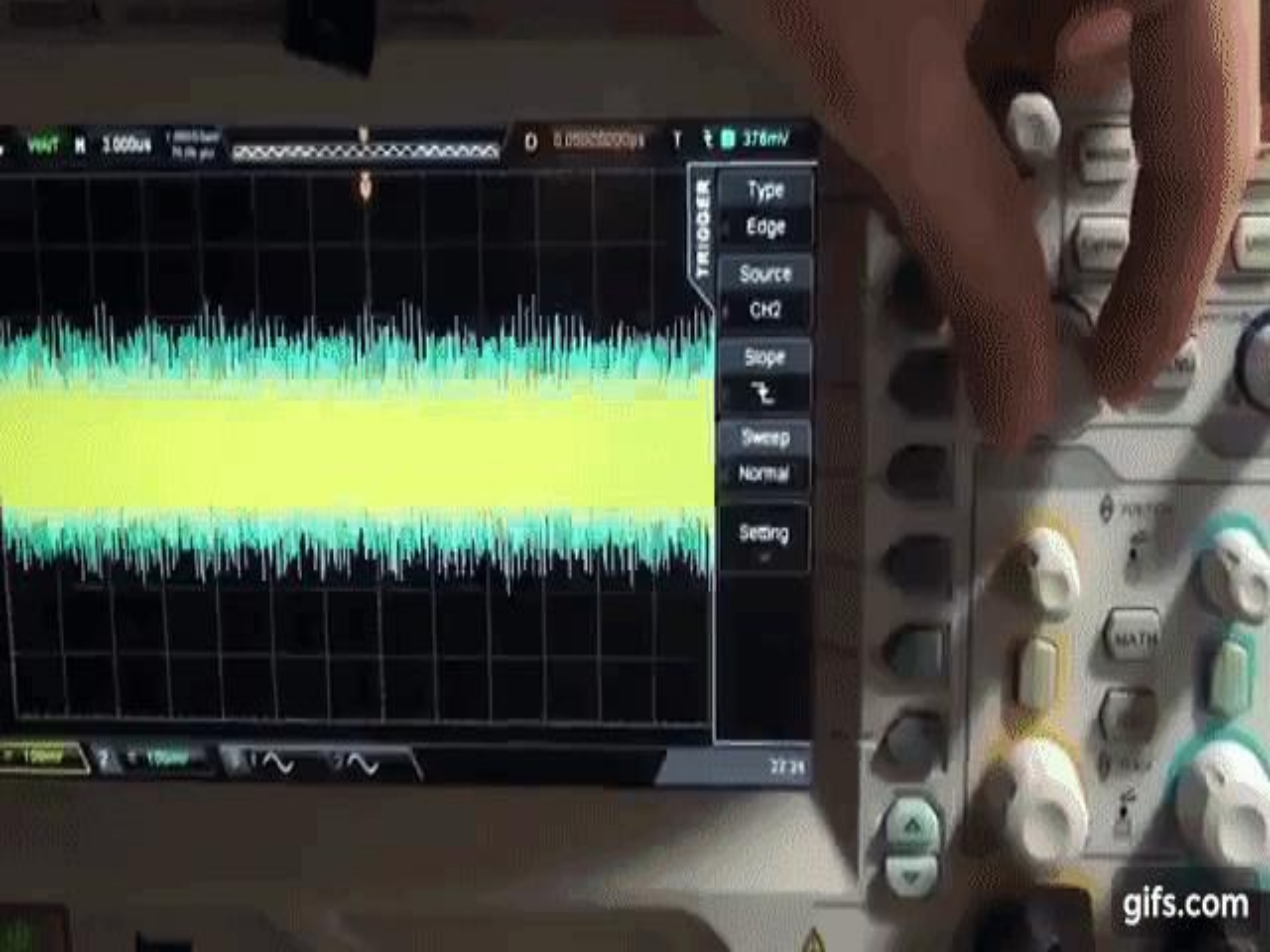
Utiliza sensores de calor para extrair dados e informações importantes. Como por exemplo, descobrir a intensidade de uso de um computador ou servidor.

FAULT INDUCTION

Consiste em adulterar um dispositivo para que ele execute operações erradas, esperando que o resultado desse comportamento errôneo possa vazar informações sensíveis.

Power Analysis Attack

Um ataque de análise de energia se baseia no fato do invasor estudar o consumo de energia de um dispositivo físico como smart cards, ou circuito integrado.


TRIGGER
Type
Edge
Source
CH2
Slope
Sweep
Normal
Setting
MATH
gifs.com

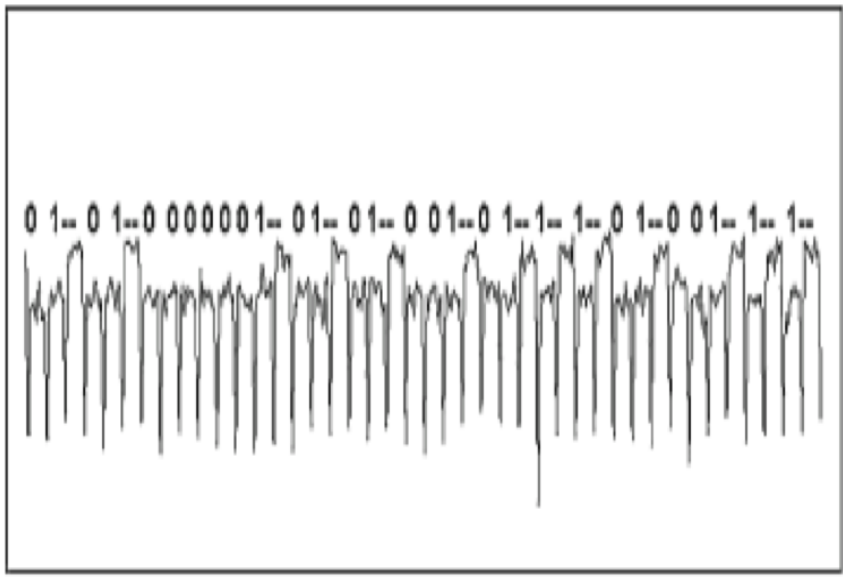
Diferentes Meios de Ataque

• Simple Power Analysis (SPA) – Envolve a interpretação visual de traços de energia ao longo do tempo, já que as variações de energia ocorrem de modo diferente para cada operação, podendo verificar qual ação está sendo executada e representando informações internas sobre uma chave criptográfica do dispositivo.

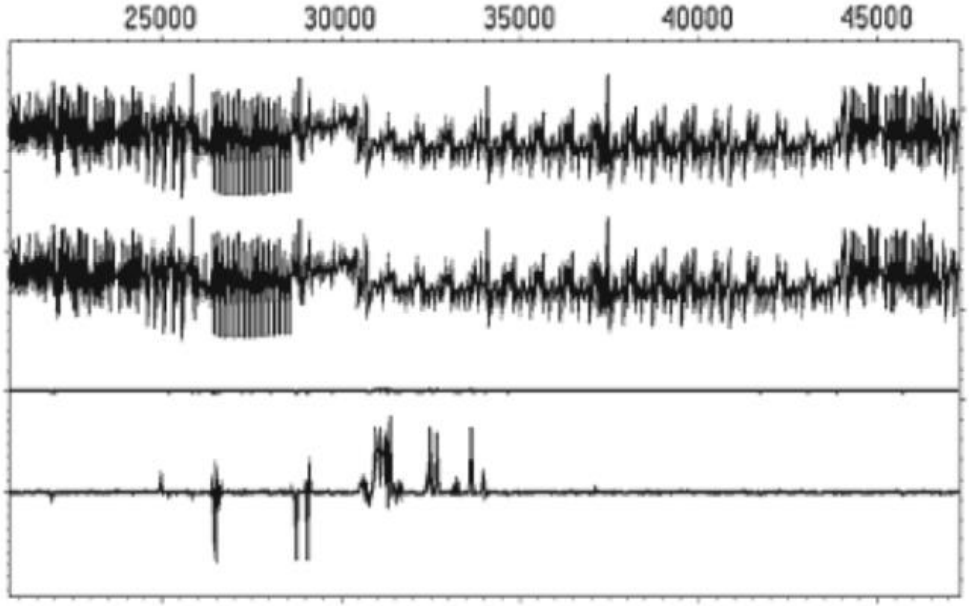
• Differential Power Analysis (DPA) – Este meio usa variações do consumo de energia de um sistema criptográfico, analisando os bits de dados individuais de acordo com a operação, para a recomposição de uma chave criptográfica.

Análise SPA x DPA

SPA



DPA

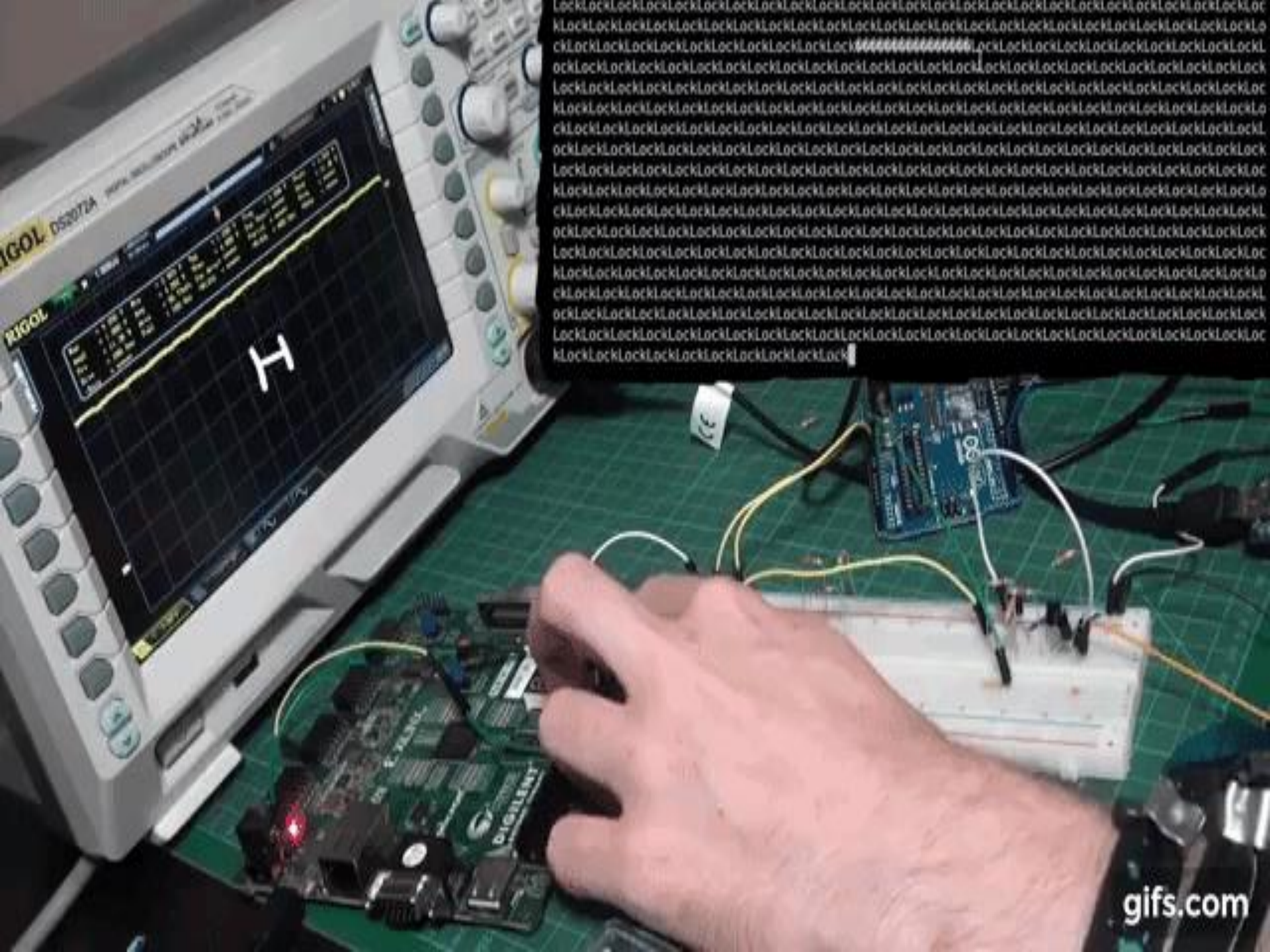


Fault Induction Attack

Se refere ataque de indução a falha um ataque onde é utilizado técnicas para definir ou redefinir qualquer bit individual de dispositivos, podendo também interromper o fluxo de controle do processador, ou onde a iluminação de um transistor alvo faz com que ele seja induzido a uma falha.

Aplicação

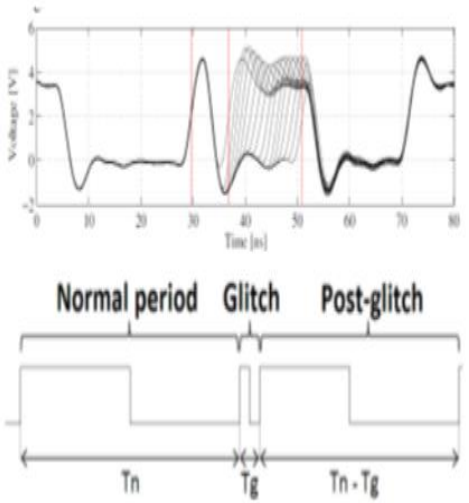
Até agora, a técnica mais amplamente conhecida para induzir esta falha é a introdução de transientes (surto de tensão elétrica num intervalo de tempo muito curto) na linha de energia ou clock do chip alvo.


RIGOL
RIGOL
H
DIGILENT
gifs.com

Métodos

Não Invasivo

Sem dano físico ao dispositivo, modifica a condição de execução do dispositivo com um conhecimento e equipamento moderado, na maioria das vezes de baixo custo ou improvisados.

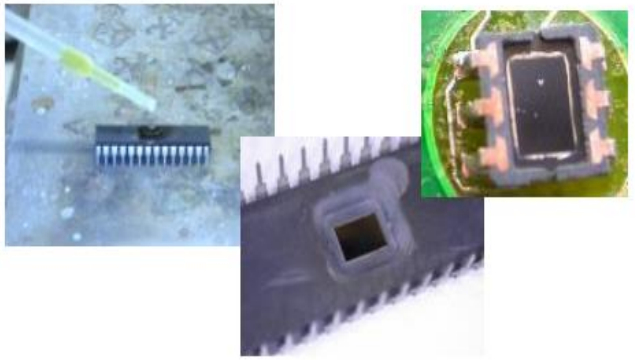


Métodos

Semi Invasivo

Descapsulação de chips, removendo camadas de metal por ácido ou corte específico, sendo necessário o uso de equipamento adequado.

AirClean Systems



Métodos

Invasivo

Estabelecendo contato elétrico com o chip, havendo a modificação ou mesmo a destruição do dispositivo, é necessário o uso de equipamento de alto custo como aparelhos para diagnóstico de semicondutores.

src: ZEISS

src: Bridge Technology

Oh e agora?? O que devo fazer??

Prevenção

● **Ofuscação** – Manter o algoritmo em segredo forçando o atacante a aplicar engenharia reversa junto com a análise de energia.

● **Introdução ao Ruído** – São aplicadas técnicas para adicionar diferentes tipos de ruído, prejudicando as medições de consumo de energia durante uma ação.

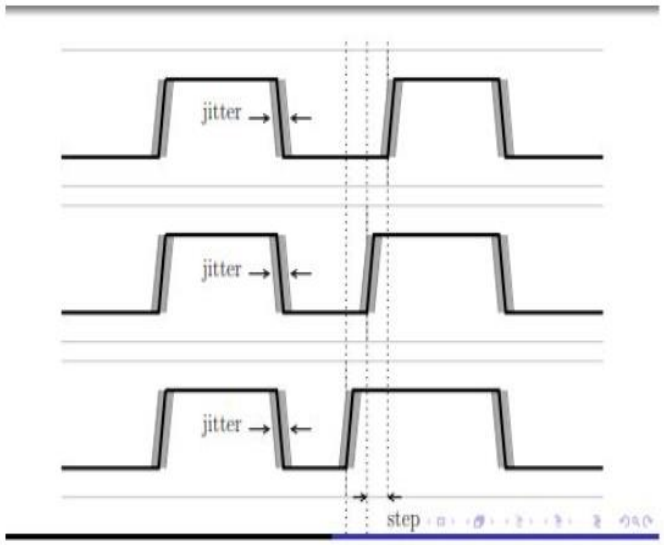
● **Energia Estável** – Embora não seja possível manter uma energia padrão para cada execução de um dispositivo, é possível implementar técnicas que reduzem estas variações durante as diferentes ações.

● **Aleatoriedade** – Inclui técnicas para randomizar os dados manipulados pelo dispositivo, de uma forma que ainda produza o resultado correto, englobando técnicas de mascaramento ou ocultação de dados e chaves.

Prevenção

Muitos fabricantes de chips já implementaram defesas contra os ataques não invasivos mais óbvios.

Essas defesas incluem jitter de clock aleatório e circuitos que reagem a falhas, redefinindo o processador.



MELTDOWN

O que é o Meltdown?

Meltdown é um ataque anunciado em Janeiro de 2018 que explora os efeitos colaterais da execução fora de ordem em processadores modernos para ter acesso irrestrito a informações de qualquer posição de memória, às quais pode incluir **informações pessoais** e **senhas**.

Principais características do Meltdown

- Explora diversos side-channels, mas principalmente a memória cache e tempo de processamento.

- Permite ao atacante acesso irrestrito a qualquer dado na memória RAM.

- Afeta diversos dispositivos (Desktop, Laptop, Cloud, etc.) que utilizam processadores Intel que implementem execução fora de ordem (basicamente todos fabricados a partir de 1995).

- Também alguns processadores ARM, mas nenhum AMD.

Como funciona *execução fora de ordem?*

...

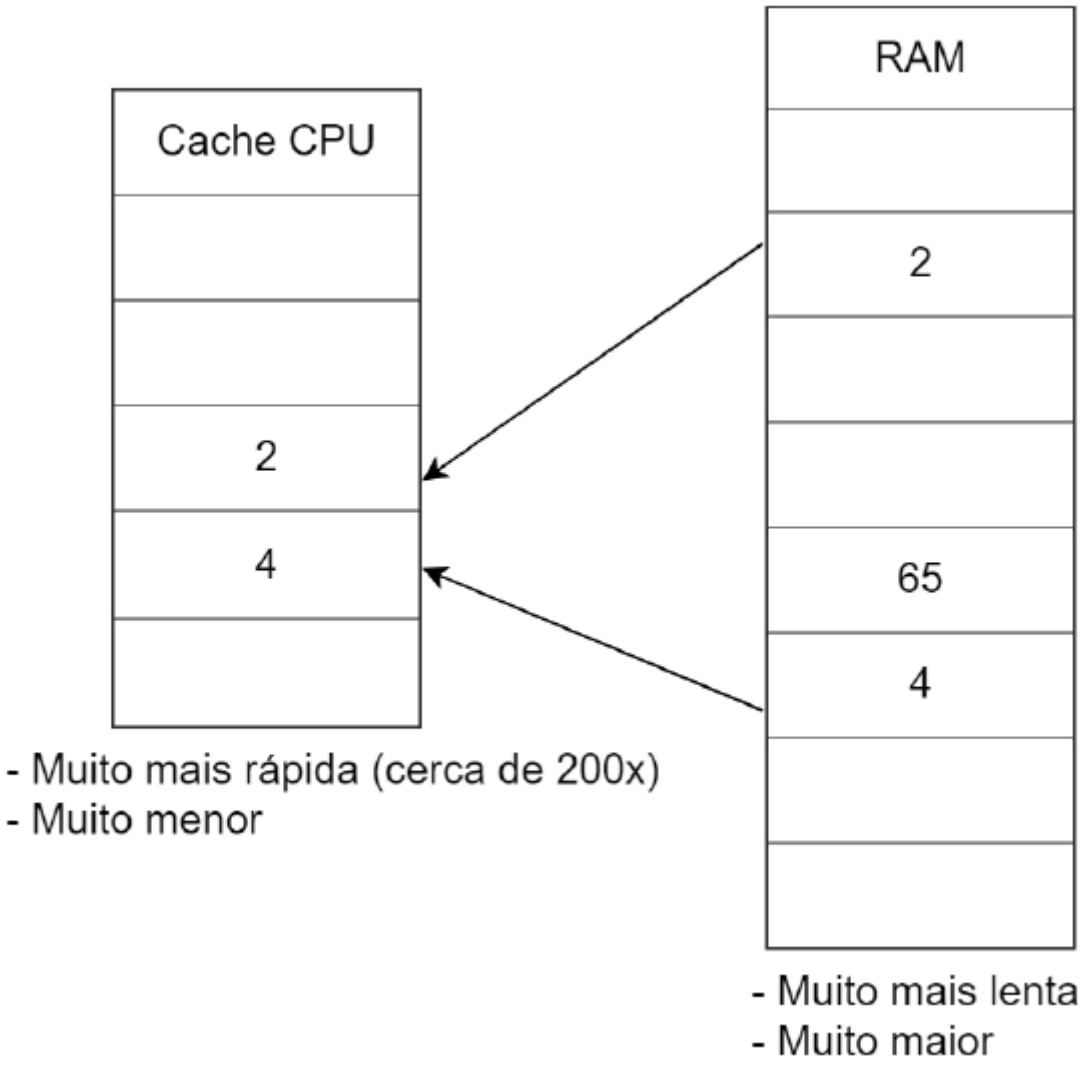
var a = 1 + 3; (1º)

var b = a + 2; (3º)

var c = 1 * 4; (2º)

...

Como funciona o cache dos processadores?



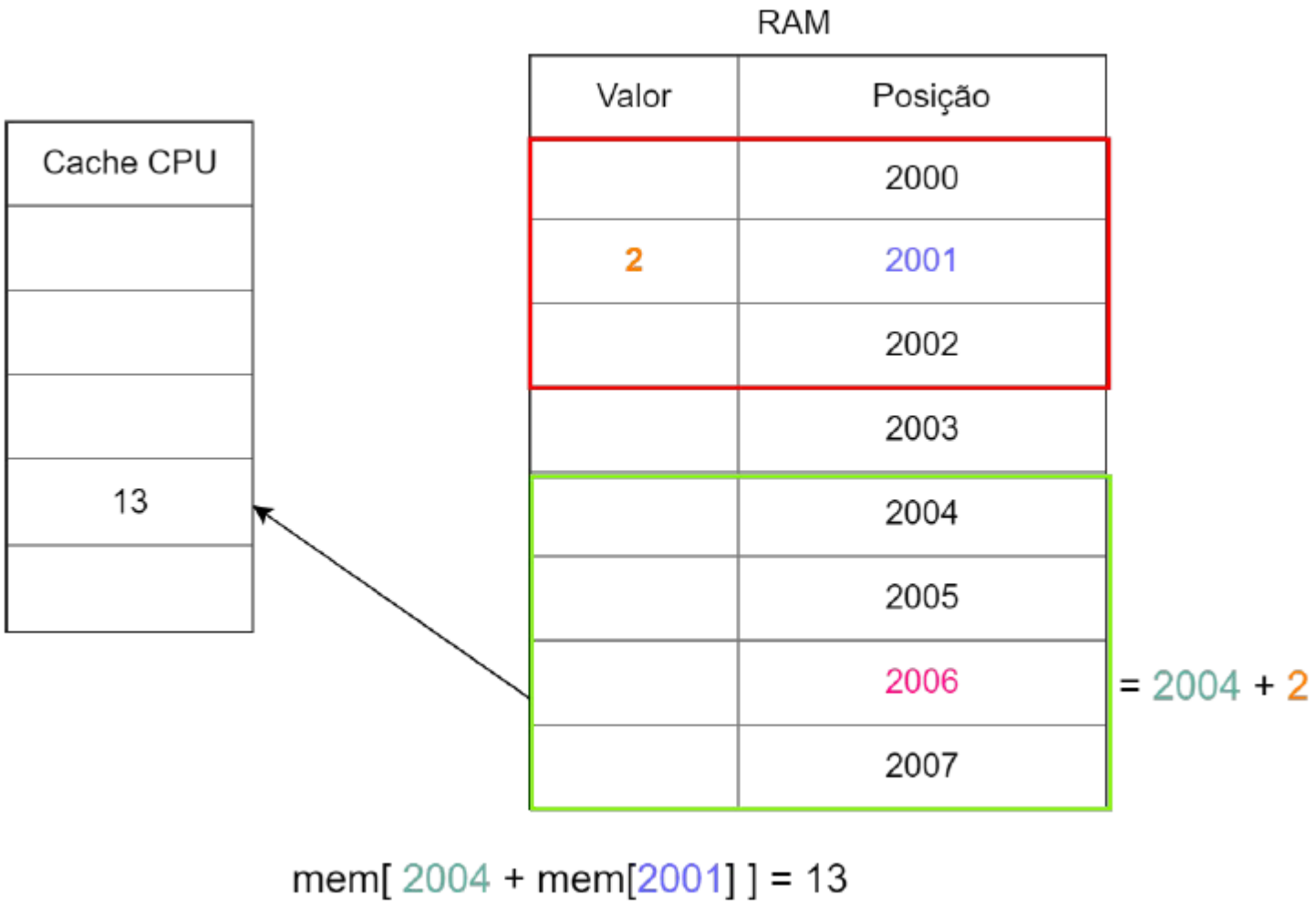
Como o Meltdown explora o cache?

Cache CPU

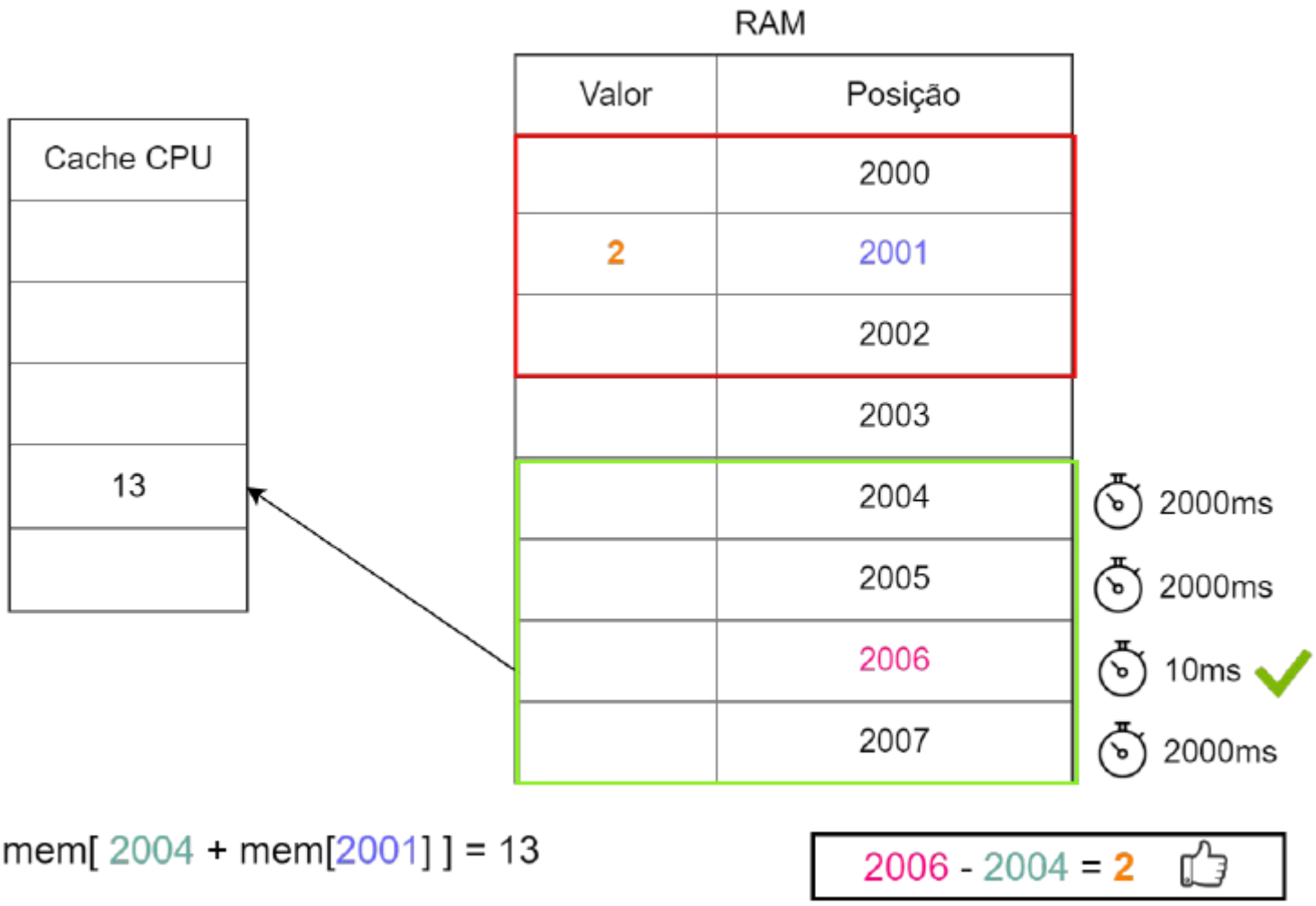
RAM

Valor	Posição
	2000
2	2001
	2002
	2003
	2004
	2005
	2006
	2007

Como o Meltdown explora o cache?

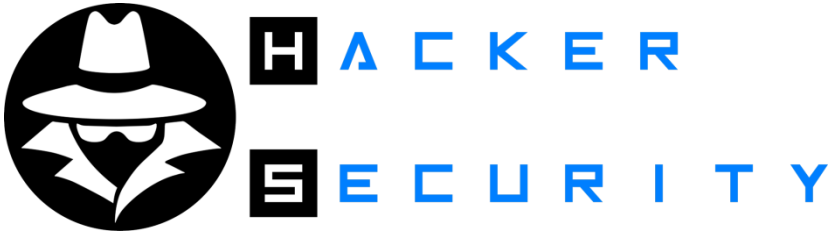


Como o Meltdown explora o cache?



Perguntas?

Obrigado!



https://www.facebook.com/tiago.rodeghieroSI
https://www.facebook.com/hackersecbr
tiago.dasreich@gmail.com