Flip Feng Shui: Hammering a Needle in the Software Stack

Kaveh Razavi, Ben Gras, and Erik Bosman, Vrije Universiteit Amsterdam; Bart Preneel, Katholieke Universiteit Leuven;

Cristiano Giuffrida and Herbert Bos, Vrije Universiteit Amsterdam

Luana Villwock Silva

Flip Feng Shui (FFS)

Esse método é descrevido como uma nova exploração de vetor que permite o atacante a induzir troca de bits em memória física arbitrária de forma totalmente controlada.

Flip Feng Shui (FFS)

Esse método depende de duas primitivas:

(i) A habilidade de induzir troca bits de maneira controlada (mas não pré-determinada) em páginas de memória física;

(ii) A capacidade de controlar o layout da memória física para reverter o mapeamento da página física alvo em um endereço de memoria virtual sob o controle do atacante.

Flip Feng Shui (FFS)

Os testes de ataque foram realizados em:

- Chaves públicas de OpenSSH
- Atualização de URLs de Debina/Ubuntu
- Chaves públicas confiáveis

Todas essas residentes na página de cache da maquina virtual da vítima

Contribuições

Explora-se:

- Falha de Hardware (Rowhammer bug)
- "Massagem" de memória

Torna:

- Fácil de atingir o alvo precisamente
- Confiável

Demostra-se: FFS = Rowhammer + Deduplicação de memória

Como funciona?

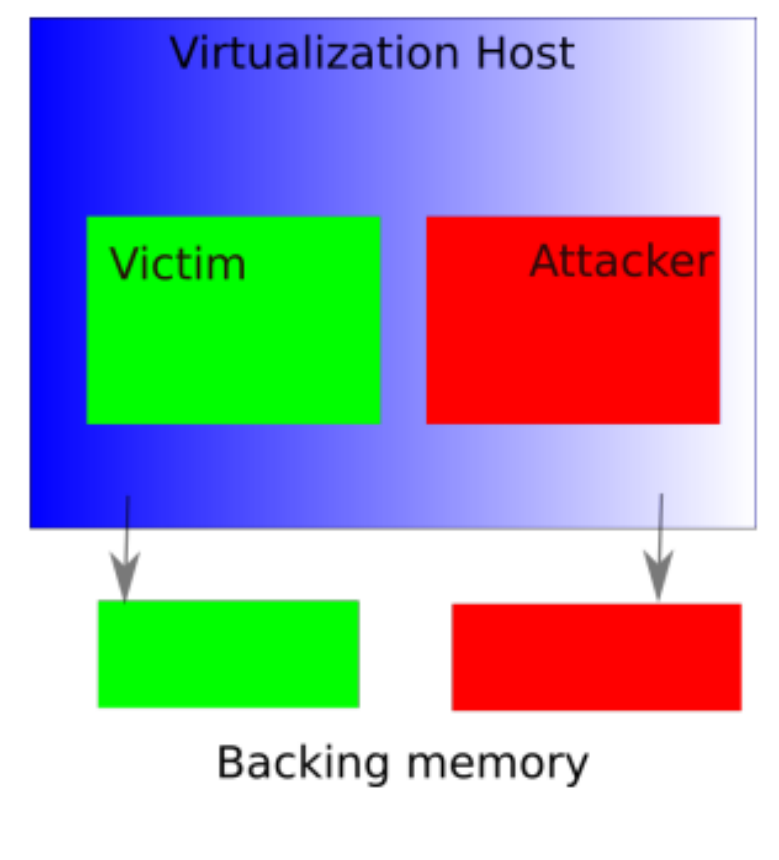
FFS transforma uma vulnerabilidade básica de hardware em uma vulnerabilidade poderosa de software através de três etapas fundamentas:

1. Memória Templating: identificação de locais na memória física que o atacante pode induzir a vulnerabilidade de hardware
2. "Massageando" memória: direcionar os dados alvos para os locais com memória física vulnerável
3. Exploração: provocar vulnerabilidade de hardware para corromper os dados destinado a exploração

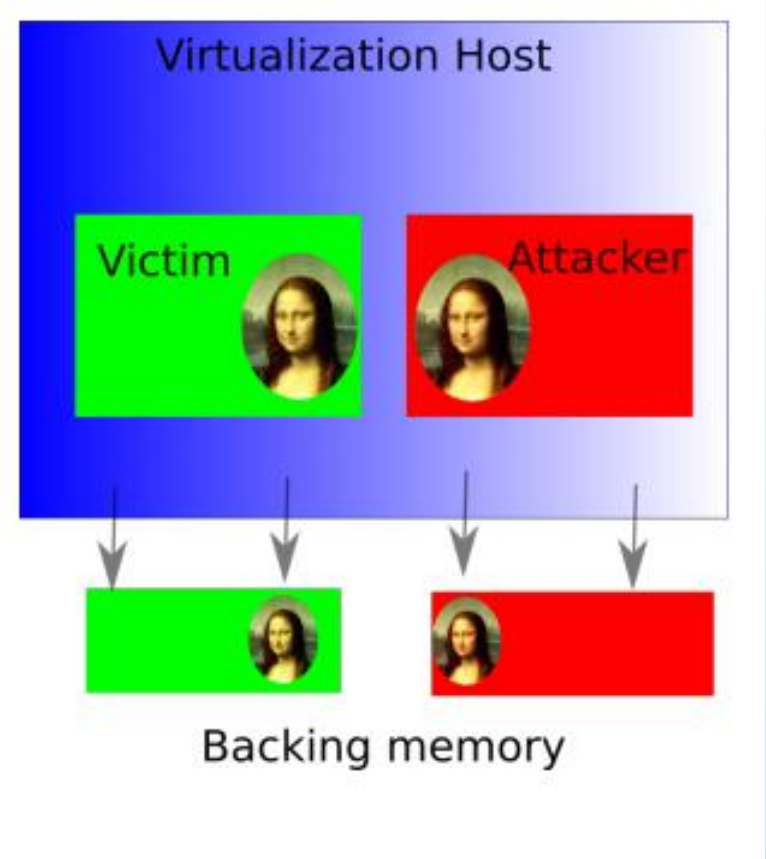
Suposições

- Co-hosted VMs
- Deduplicação de memória ligada (geralmente ligada em co-hosted VMs, pois economiza memória)
- Rowhammer (80% das DRAM acontecem esse bug)
- RSA

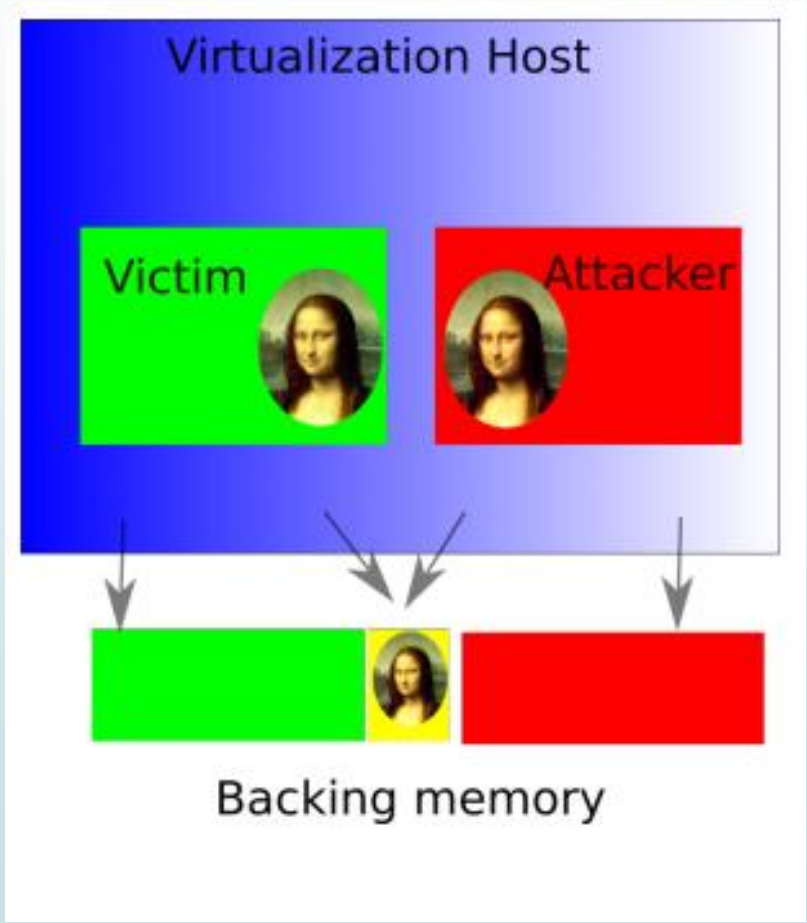
Deduplicação de memória



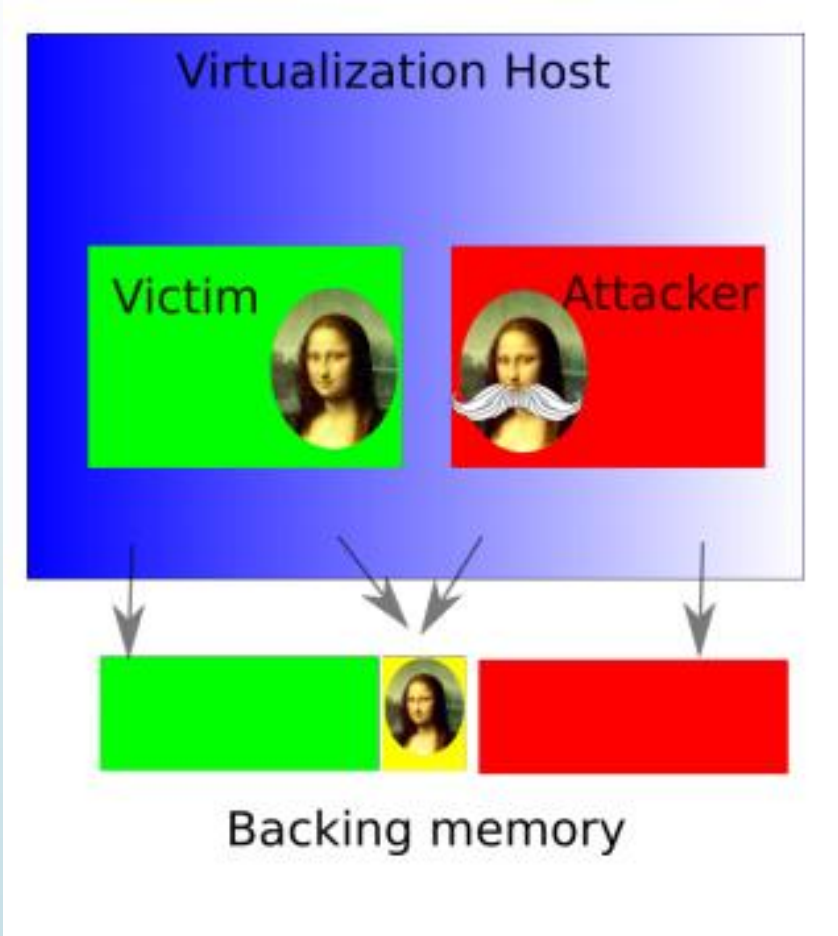
Deduplicação de memória



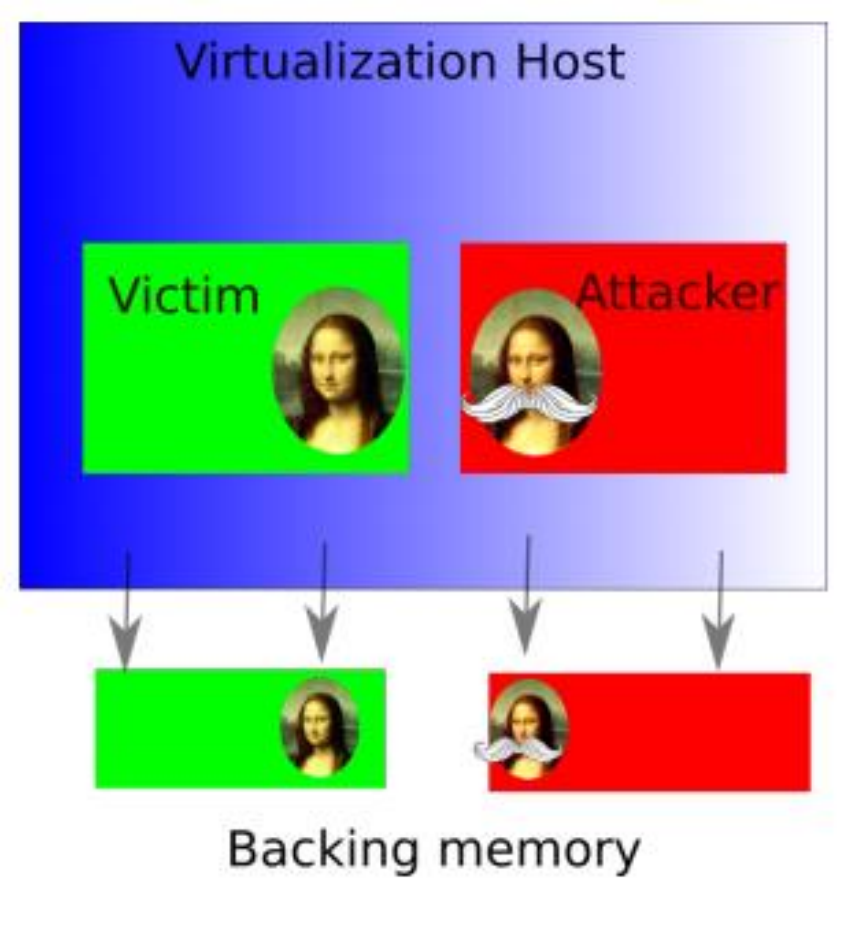
Deduplicação de memória



Deduplicação de memória

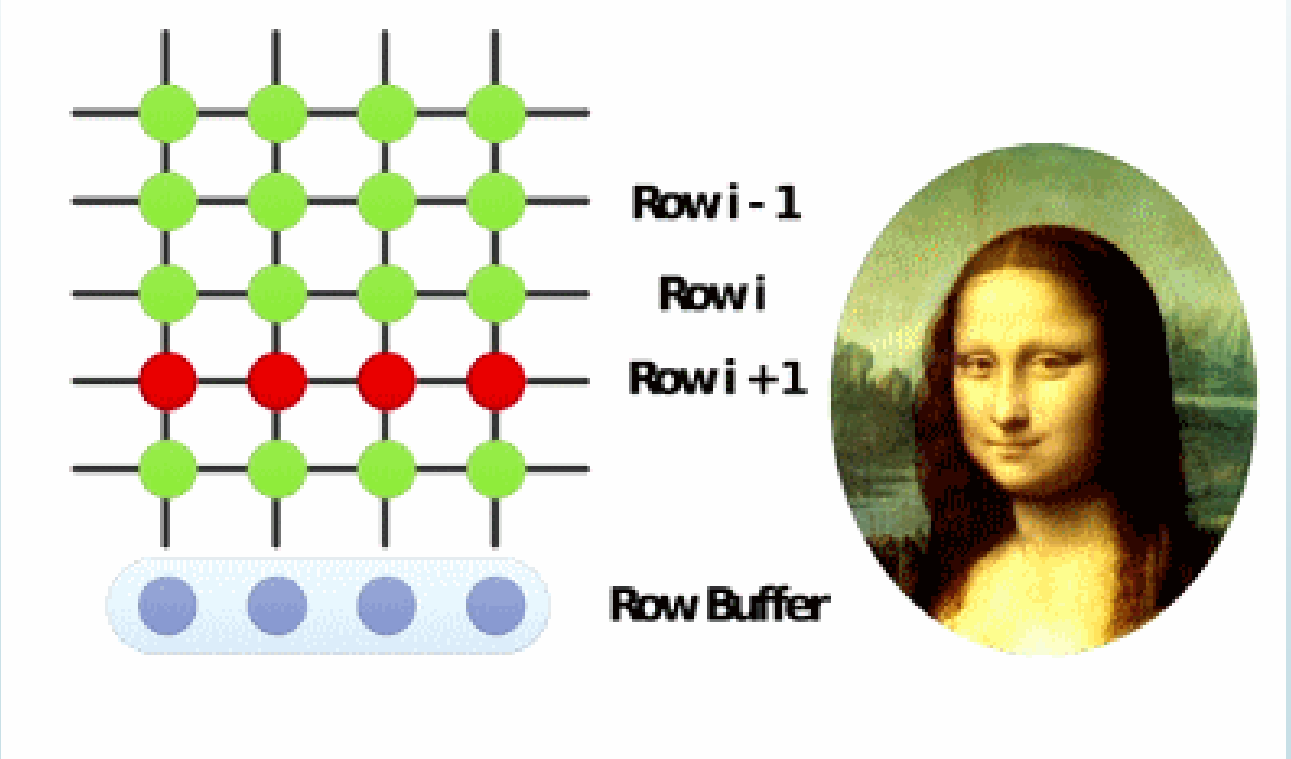


Deduplicação de memória

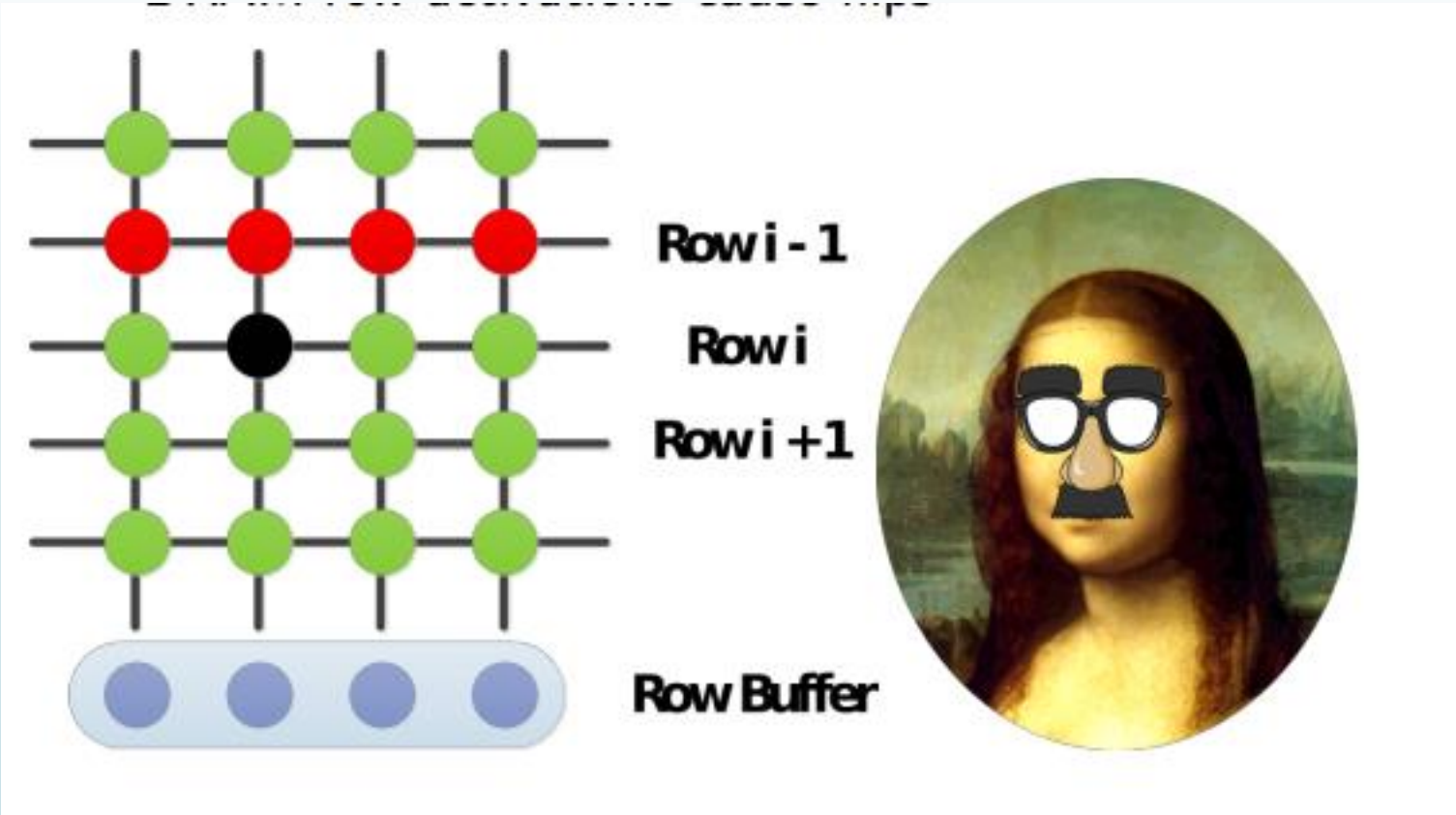


Rowhammer

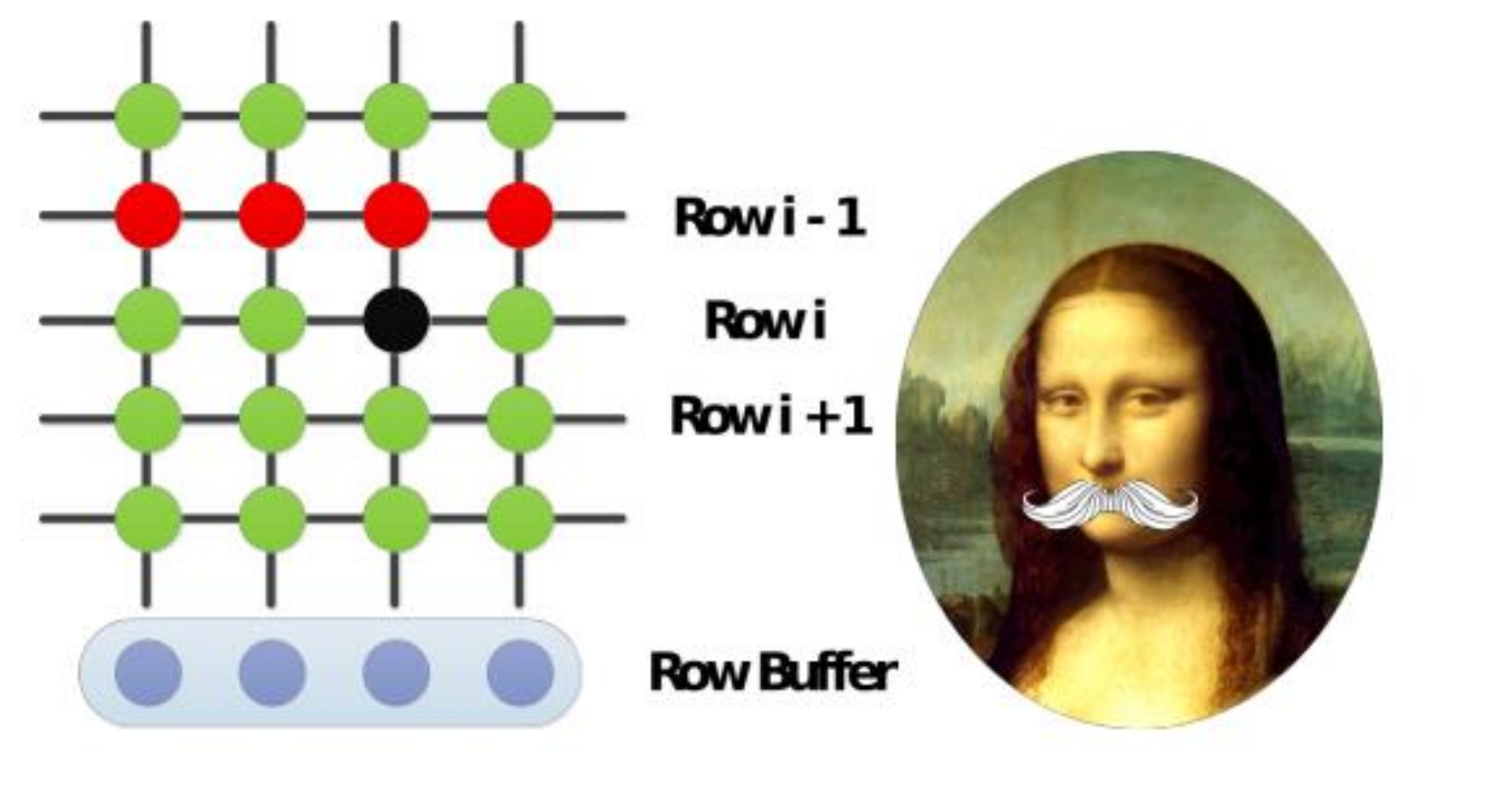
- Causa perda de energia na DRAM
- Isso causa a troca de bits



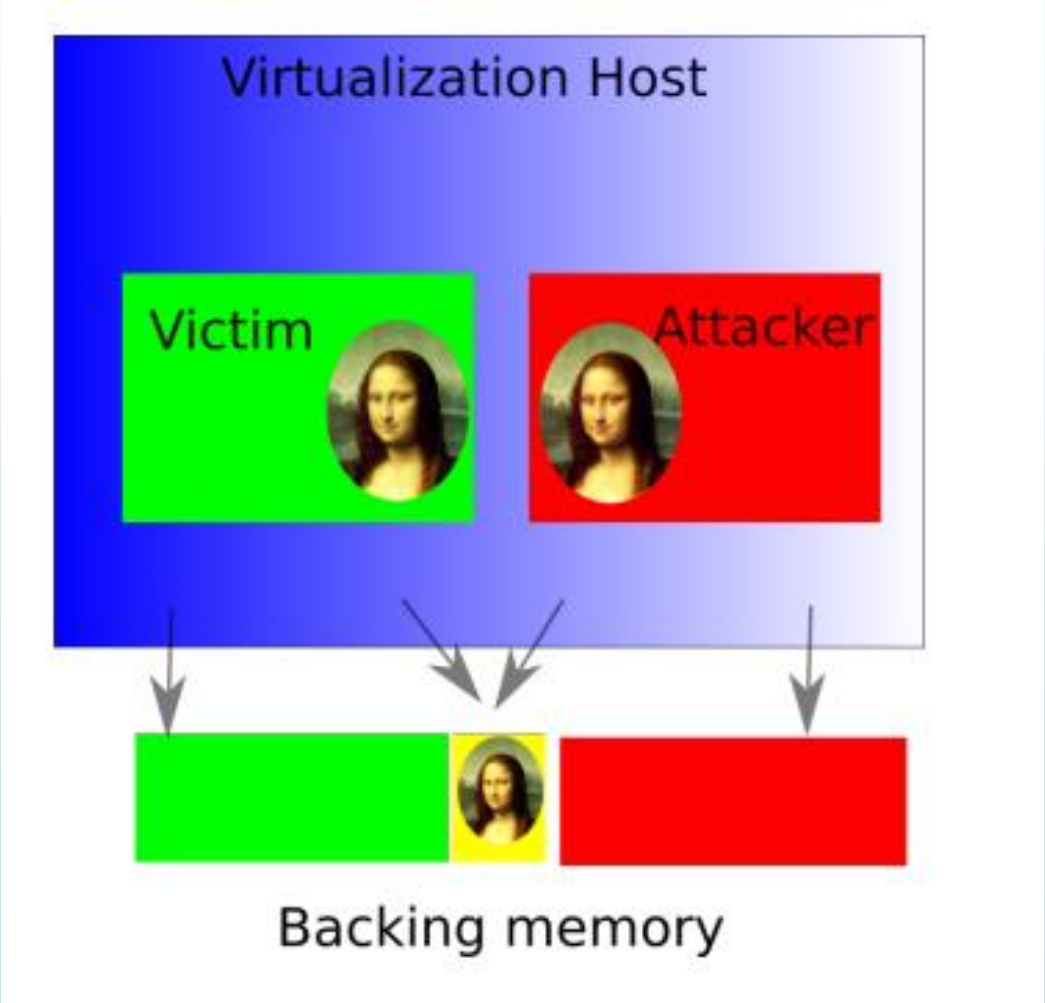
Rowhammer



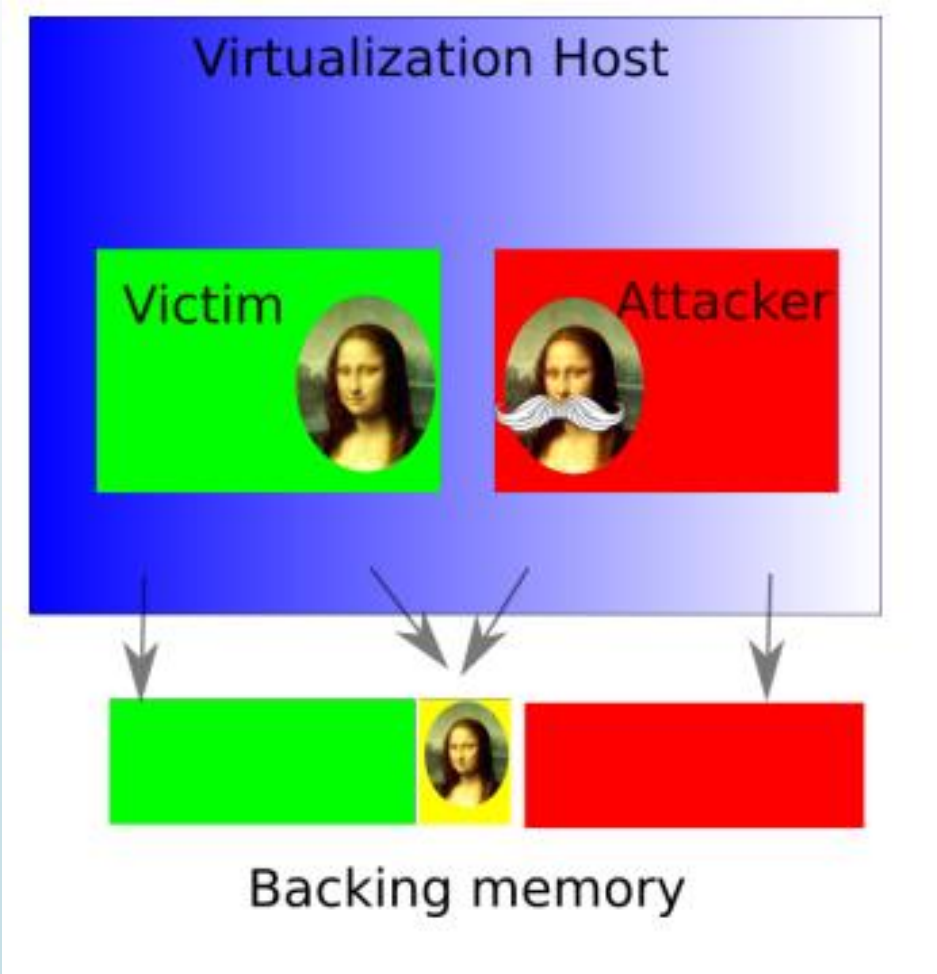
Rowhammer



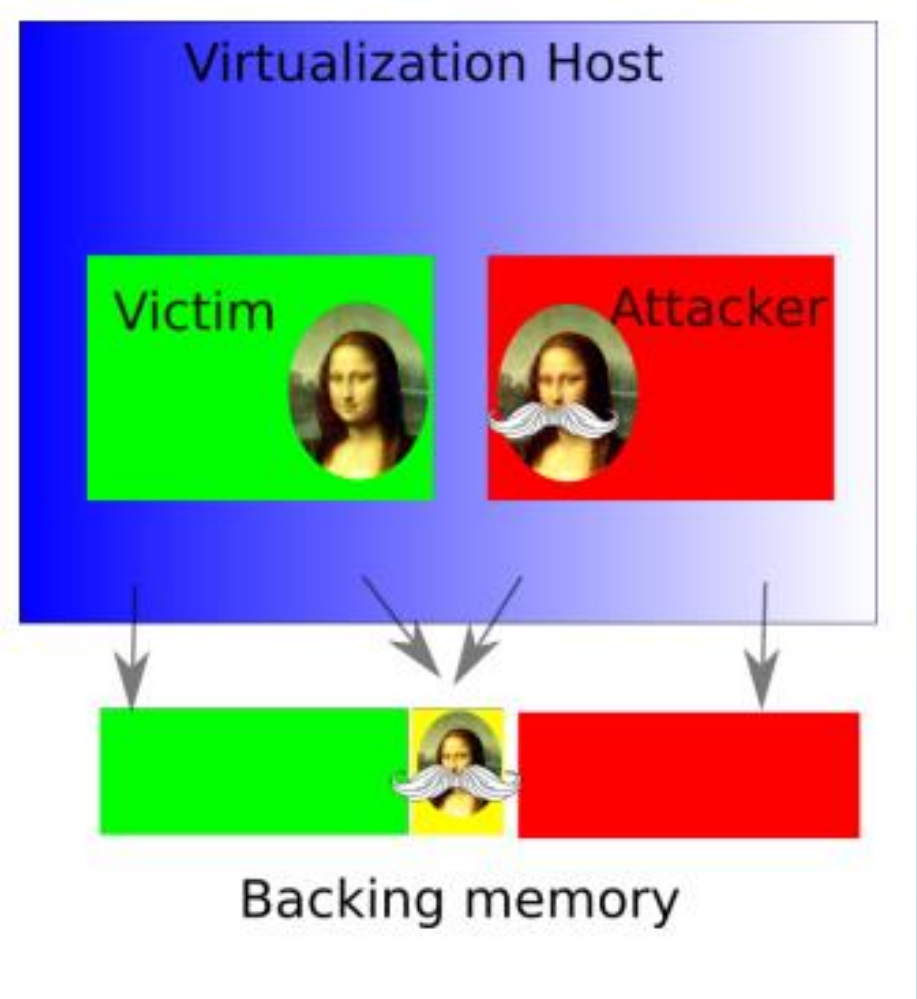
Deduplicação de memória + Howrammer = FFS



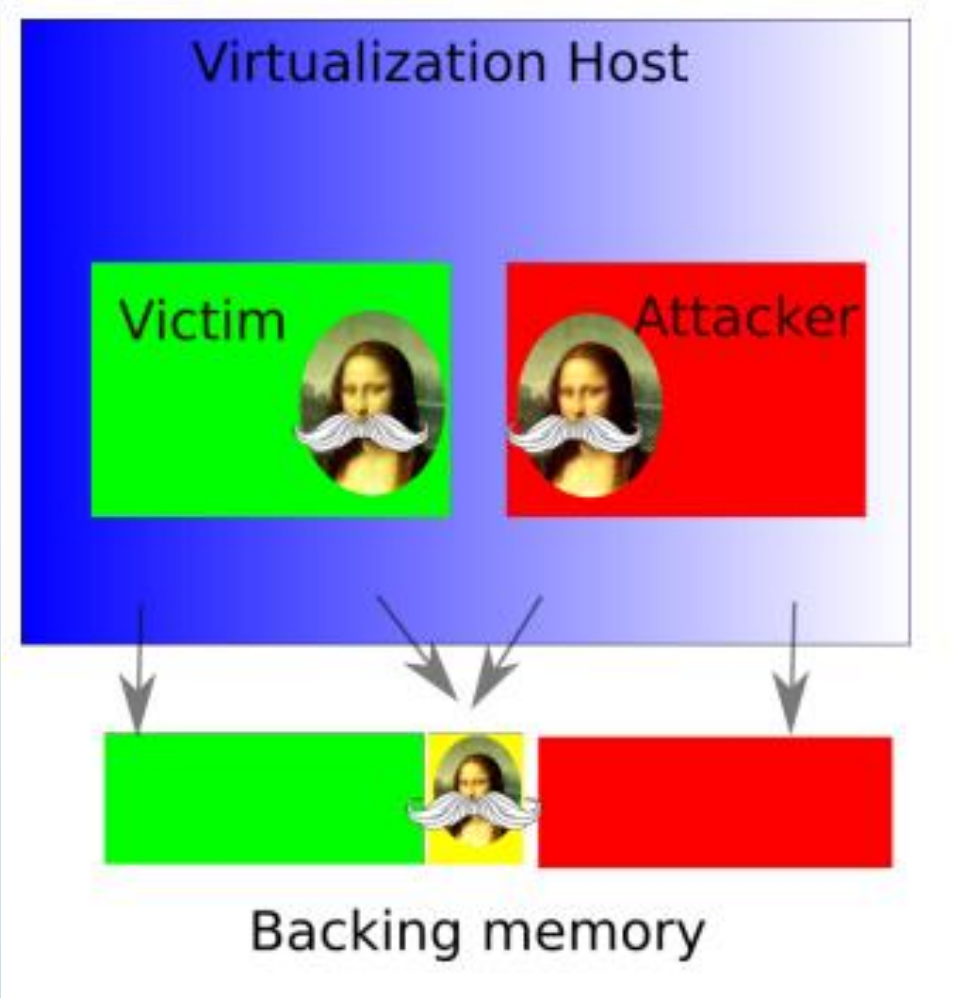
Deduplicação de memória + Howrammer = FFS



Deduplicação de memória + Howrammer = FFS



Deduplicação de memória + Howrammer = FFS

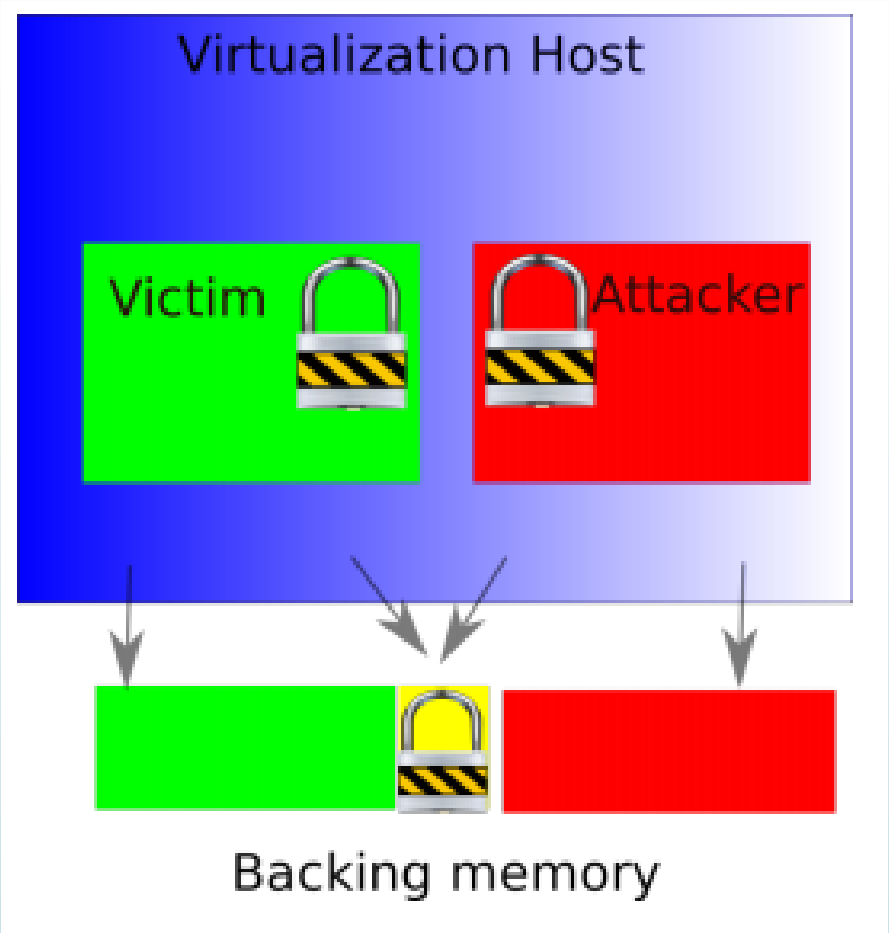


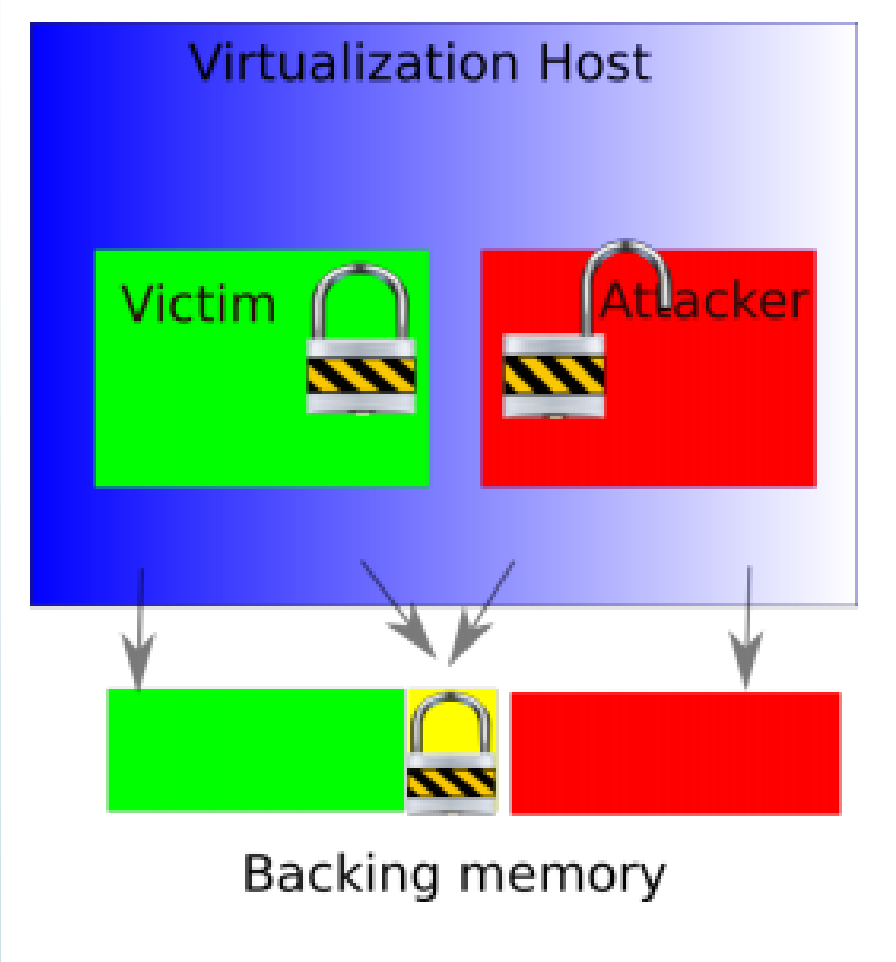
RSA

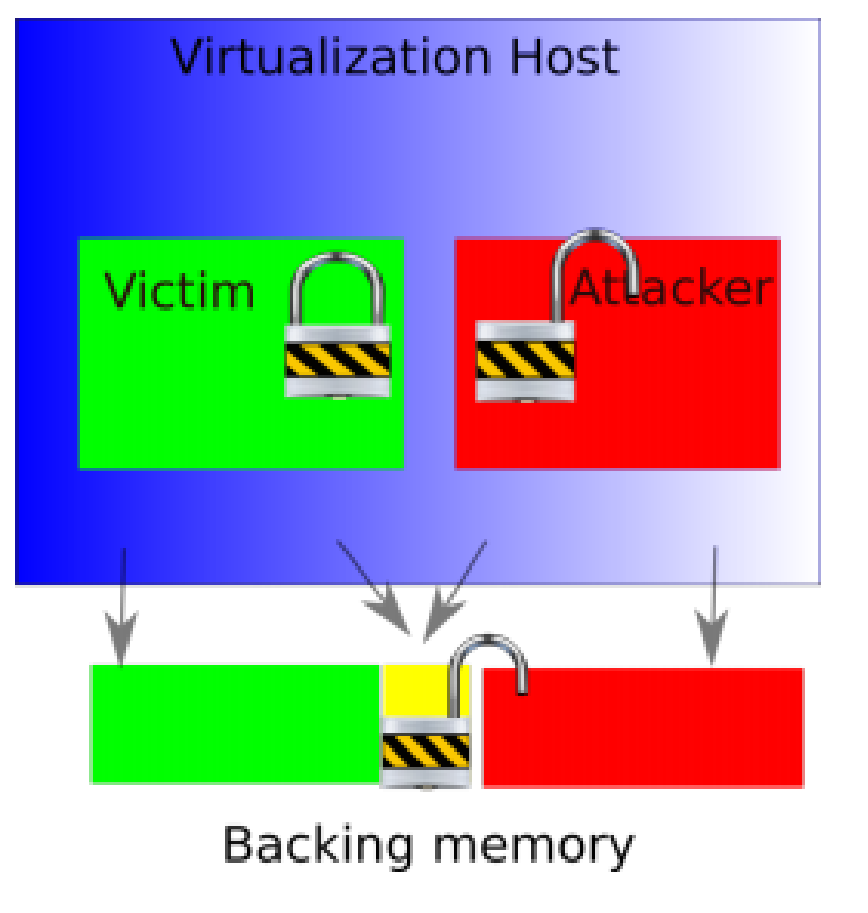
- Criptografia de chaves publicas
- Duas chaves: publicas e privadas
- Para criptografar utiliza-se a chave pública e de criptografar a privada.

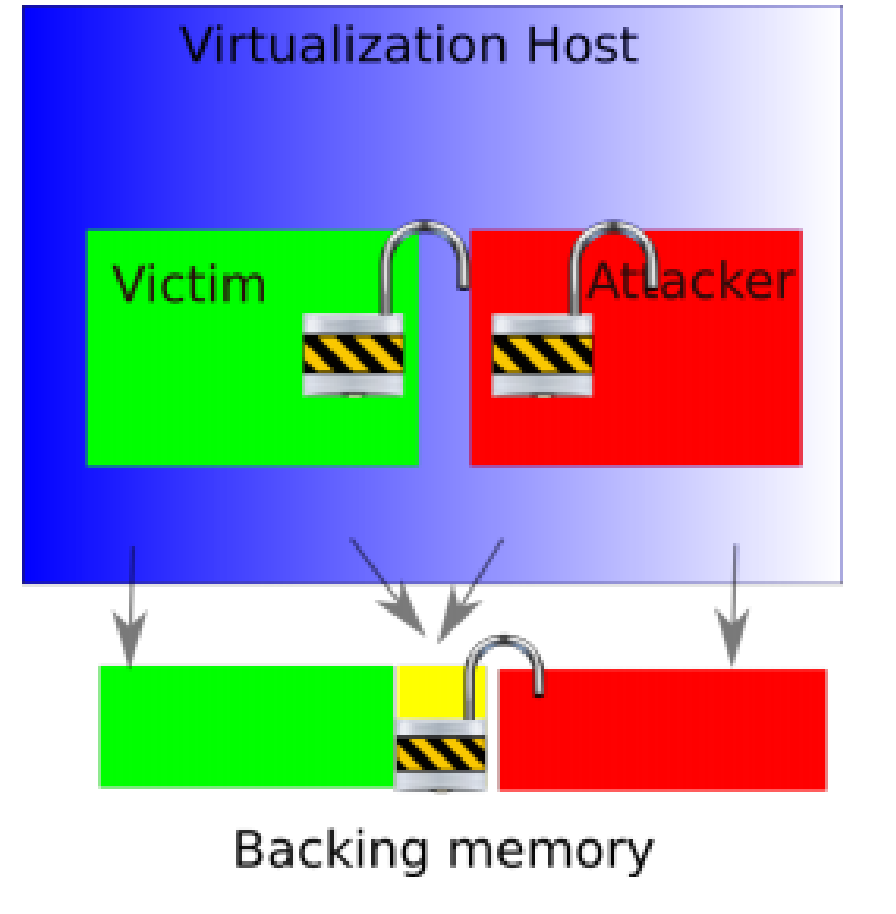
OpenSSH Attack

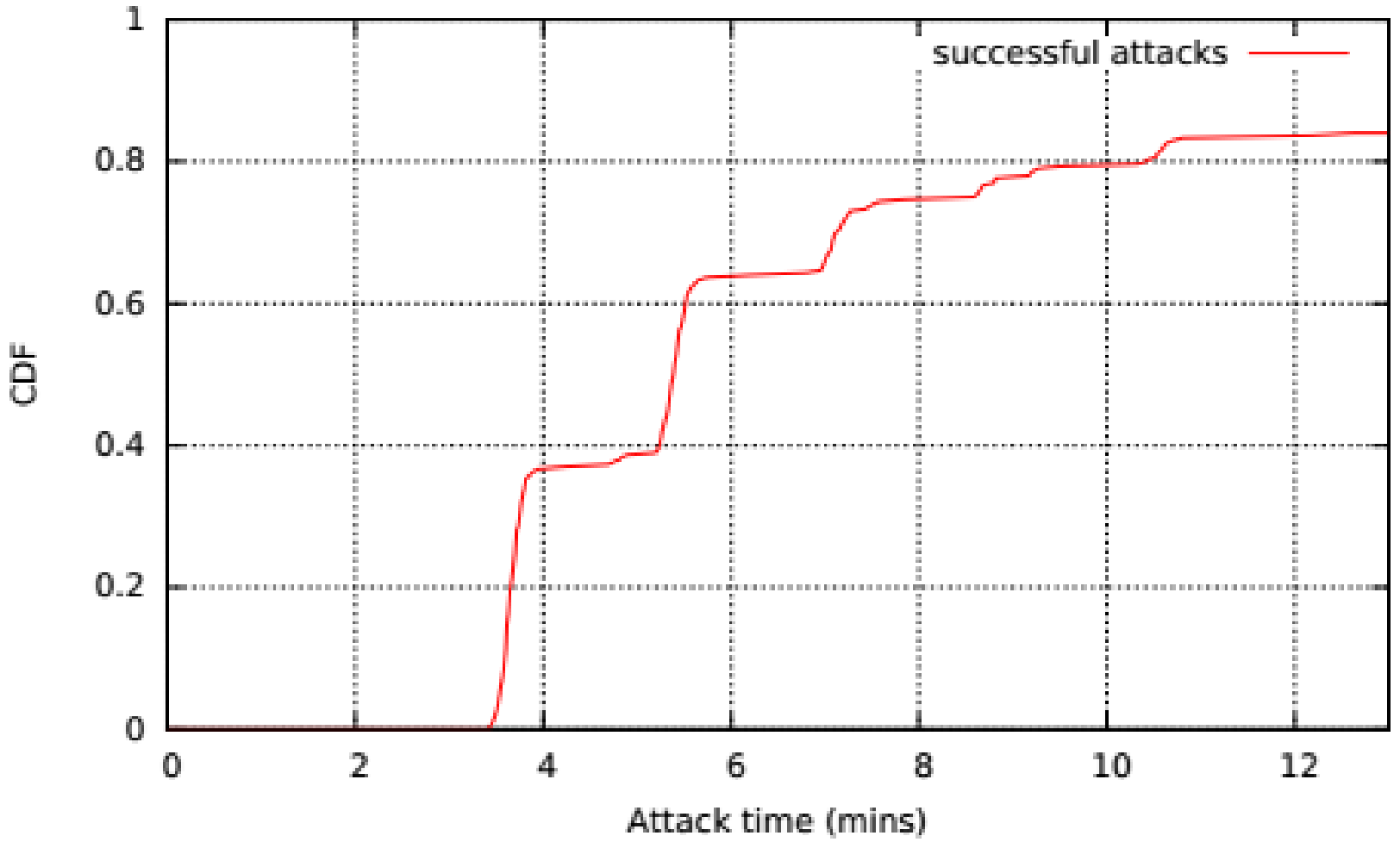
```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDX
y7MdVToVAvKBO/Xven/kqBzfRZm+GITl6sBOu+Aa
3/UTC3x+eKjB2jf+48kTP7AvsdbSwg9Q5upN77xX
3mNGwwj1RUQpOPPc99XHO9M84iCydE+9smYseySf
bJQnrov5Ricz2Z18Neuy5ZUH/Ldrf1NSwWoo5NZL
6tjOE9JvZurMPPk2EqEyHltEFC6OetJwEfaPq9kO
glmzFtBWLHR4dF1796JeVkFiWcmMaykAoN+JRF2n
MlayPlUxdWROJwxZ2cJ9la/QLXvv8xOtsORGP9ZG
5BWqOcD781evuSS3i91BNg6Osl7mlxo6Mc3oUbew
/7ddVO8WjdRBn7iQF9WN beng@mymachine
```


Virtualization Host
Victim
Attacker
Backing memory


Virtualization Host
Victim
Attacker
Backing memory


Virtualization Host
Victim
Attacker
Backing memory


Virtualization Host
Victim
Attacker
Backing memory


successful attacks
CDF
Attack time (mins)
0
0.2
0.4
0.6
0.8
1
0
2
4
6
8
10
12

Conclusão

- FFS pode quebrar isolação
- Co-hosting VM é perigoso
- Solução: Desativar memória deduplicação.

- Veja mais exemplos de ataques em: https://www.vusec.net/projects/flip-feng-shui

Referências

- Kaveh Razavi, Ben Gras, Erik Bosman, Cristiano Giuffrida and Herbert Bos; Flip Feng Shui: Hammering a Needle in the Software Stack