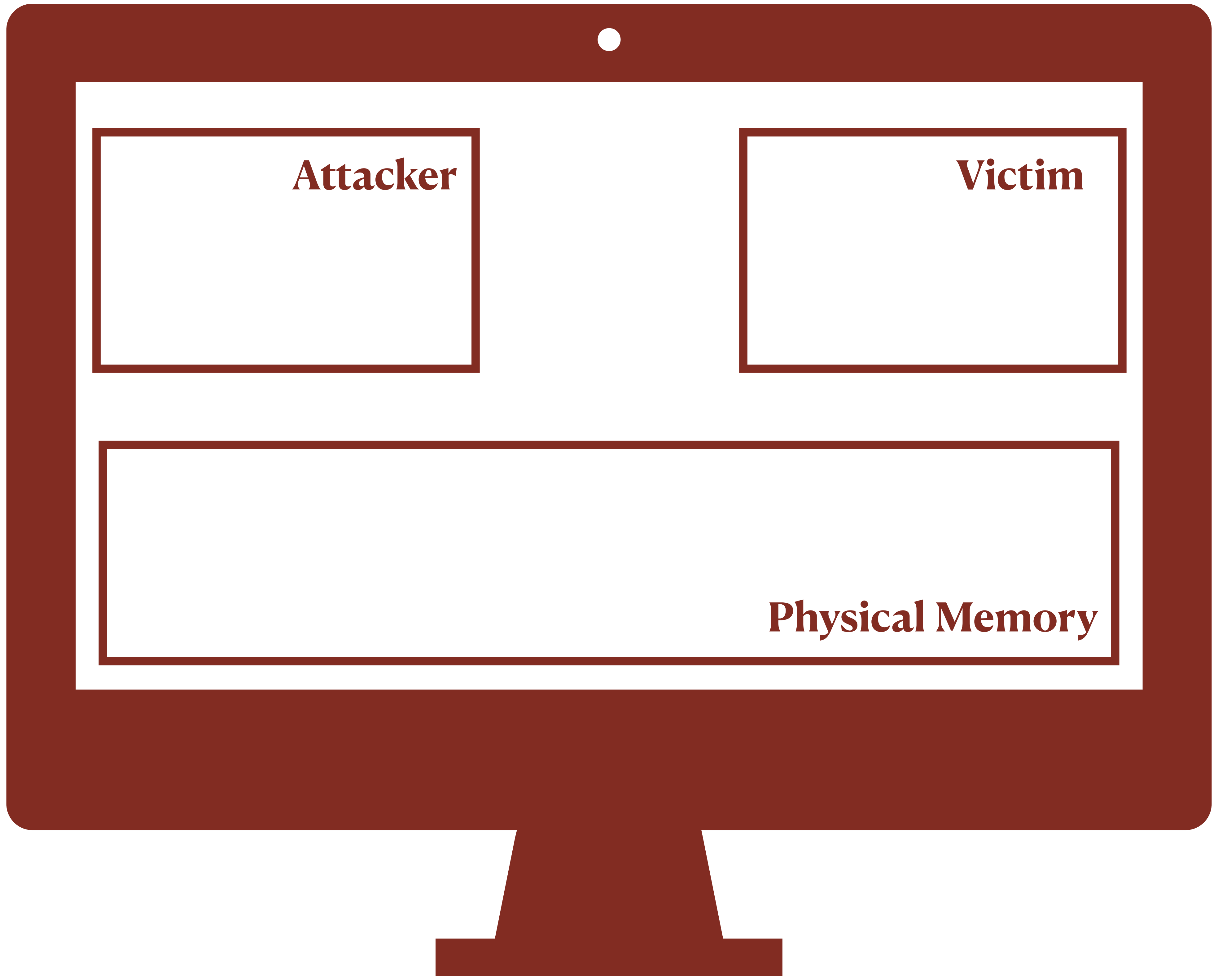
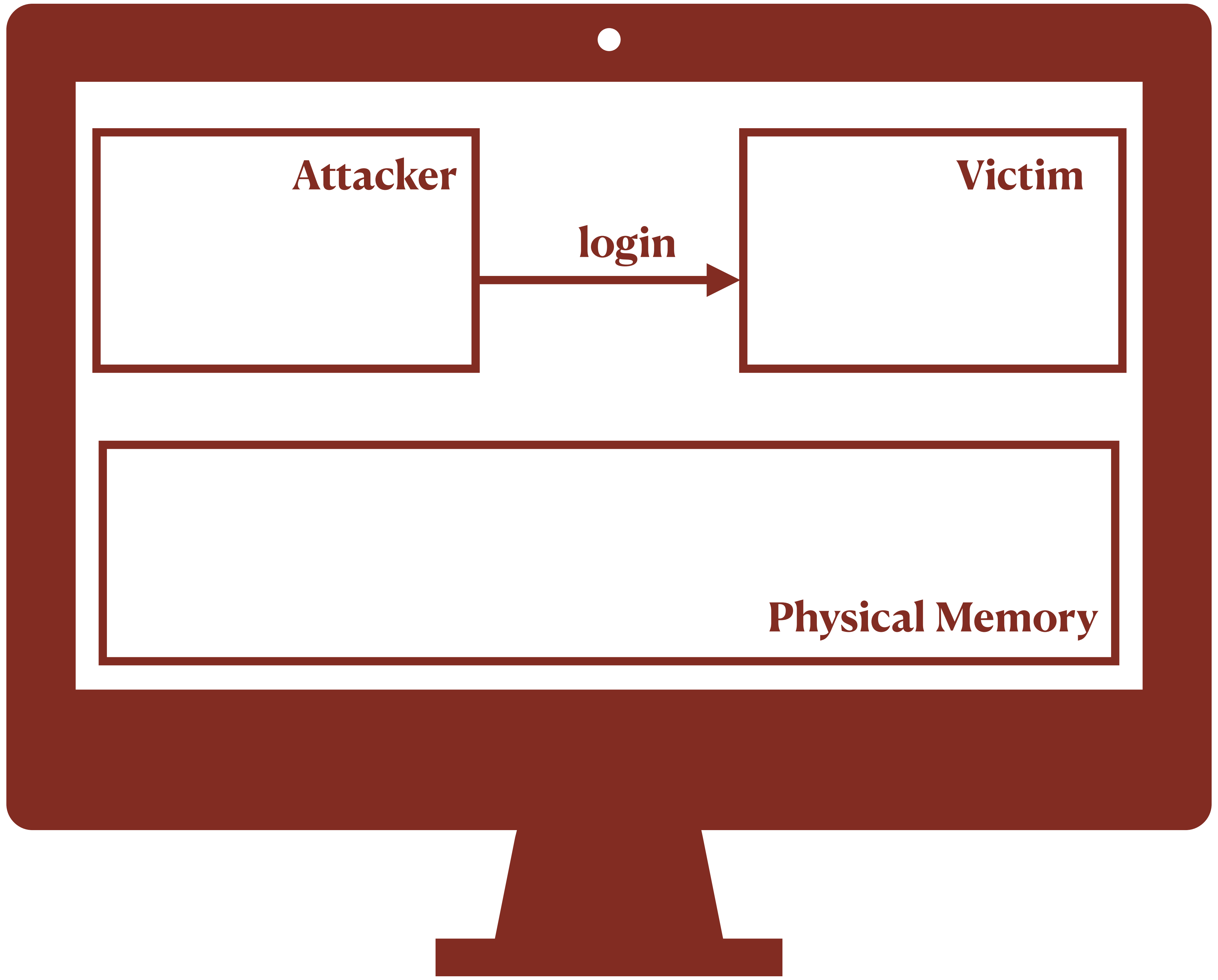
Flip Feng Shui

Kaveh Razavi*, Ben Gras*, Erik Bosman, Bart Preneel, Cristiano Giuffrida and Herbert Bos

* Equal contribution joint first authors

Presented by Daniël Trujillo
Secure Hardware Design


Attacker
Victim
Physical Memory


Attacker
login
Victim
Physical Memory

Flip

Flip

Simply a bit flip

0

Flip

Simply a bit flip

0

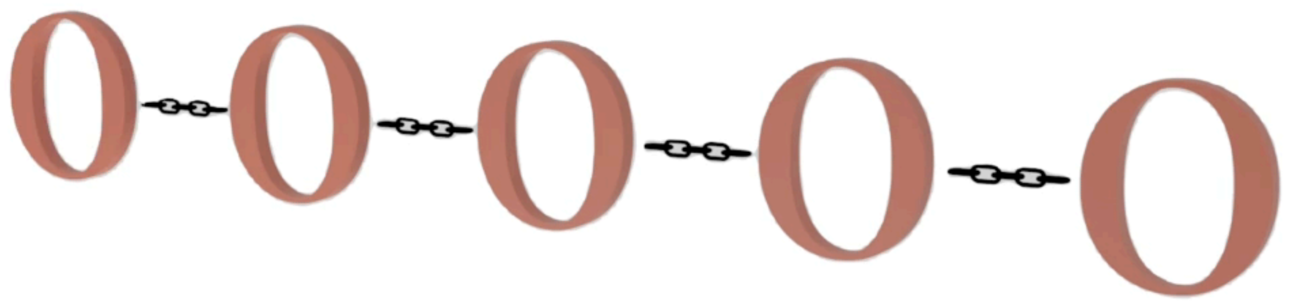
Feng Shui

Flip

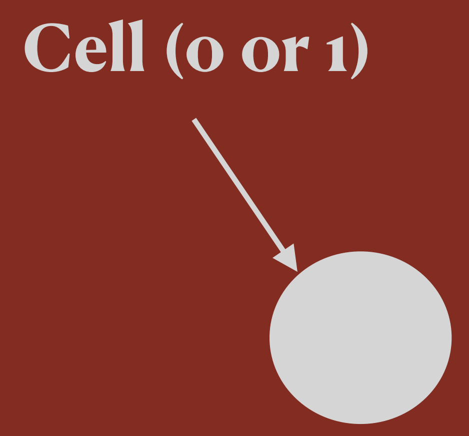
Simply a bit flip

Feng Shui

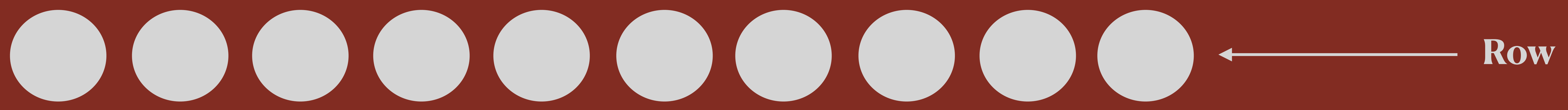
Harmonization with the environment



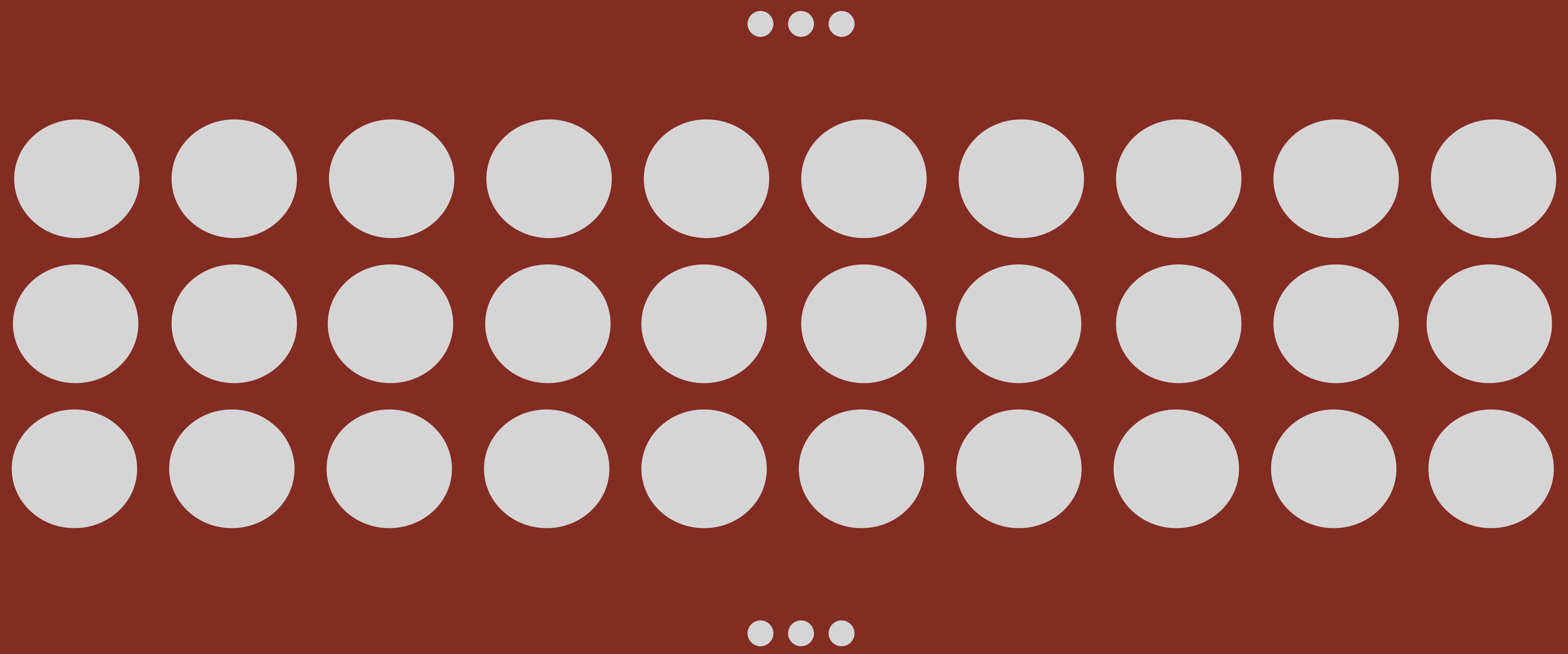
Rowhammer



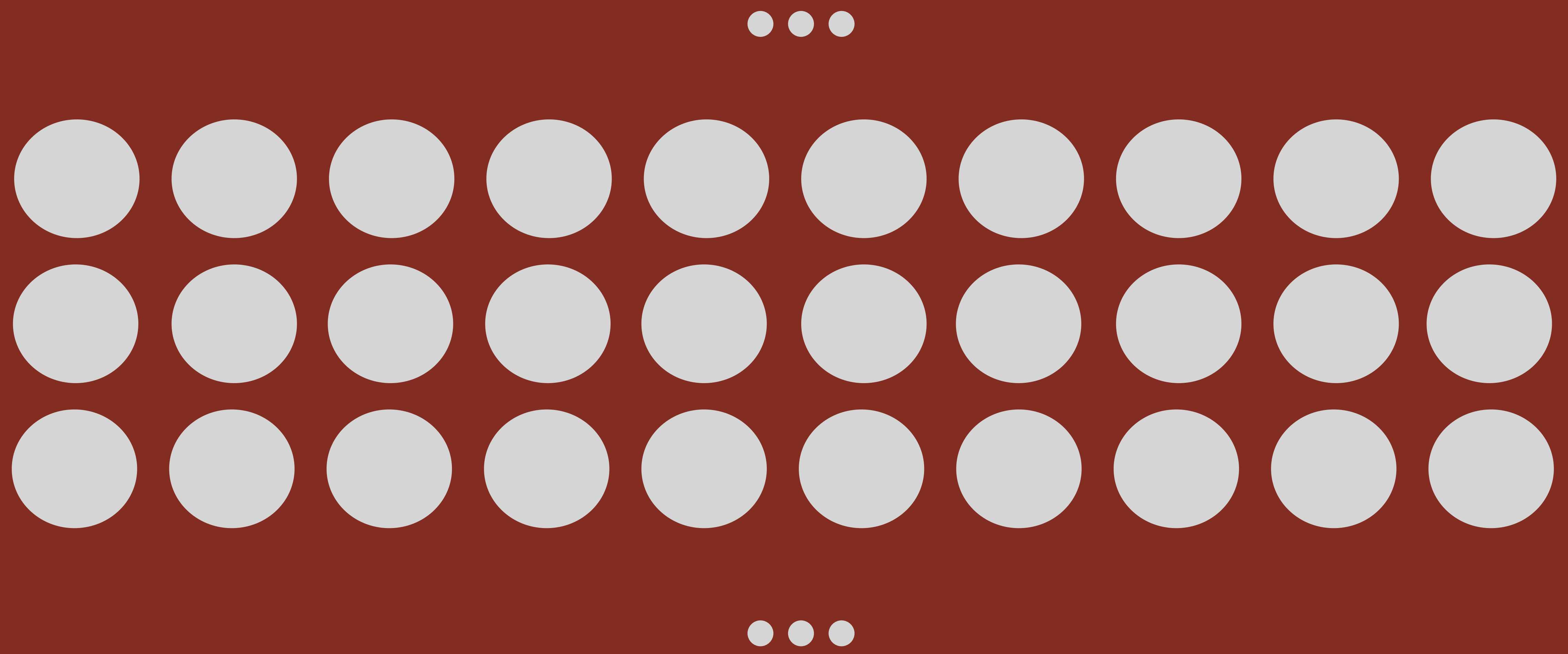
Rowhammer



Rowhammer

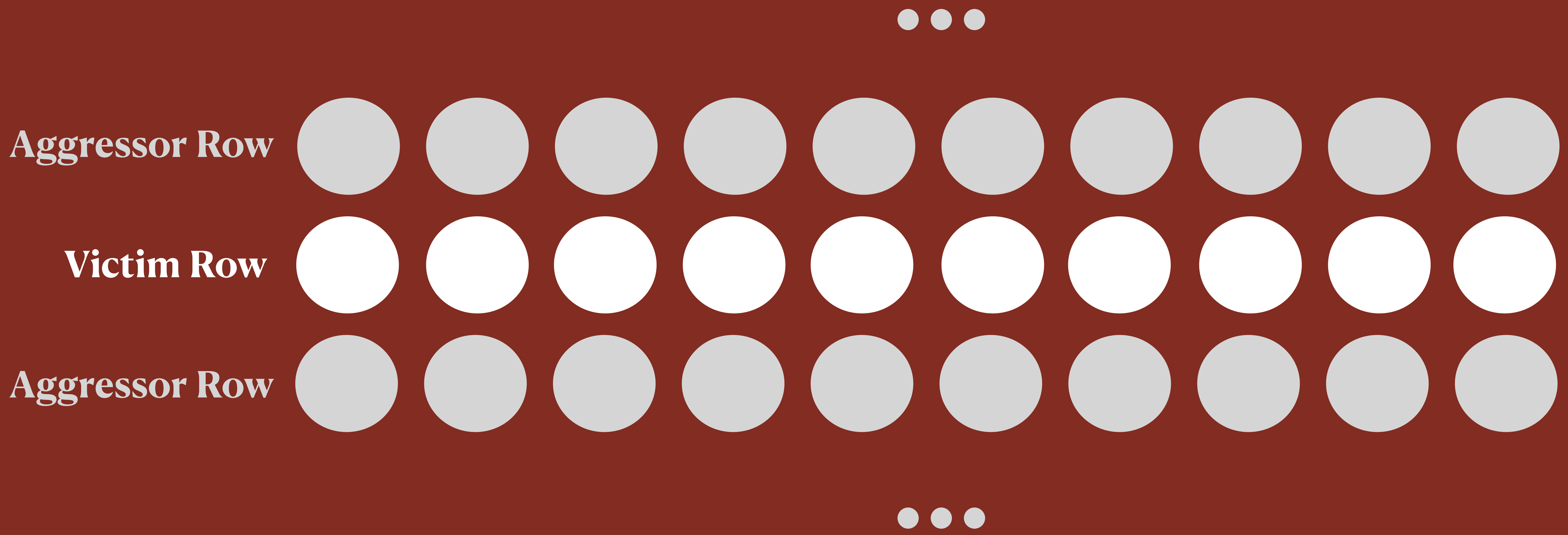


Rowhammer

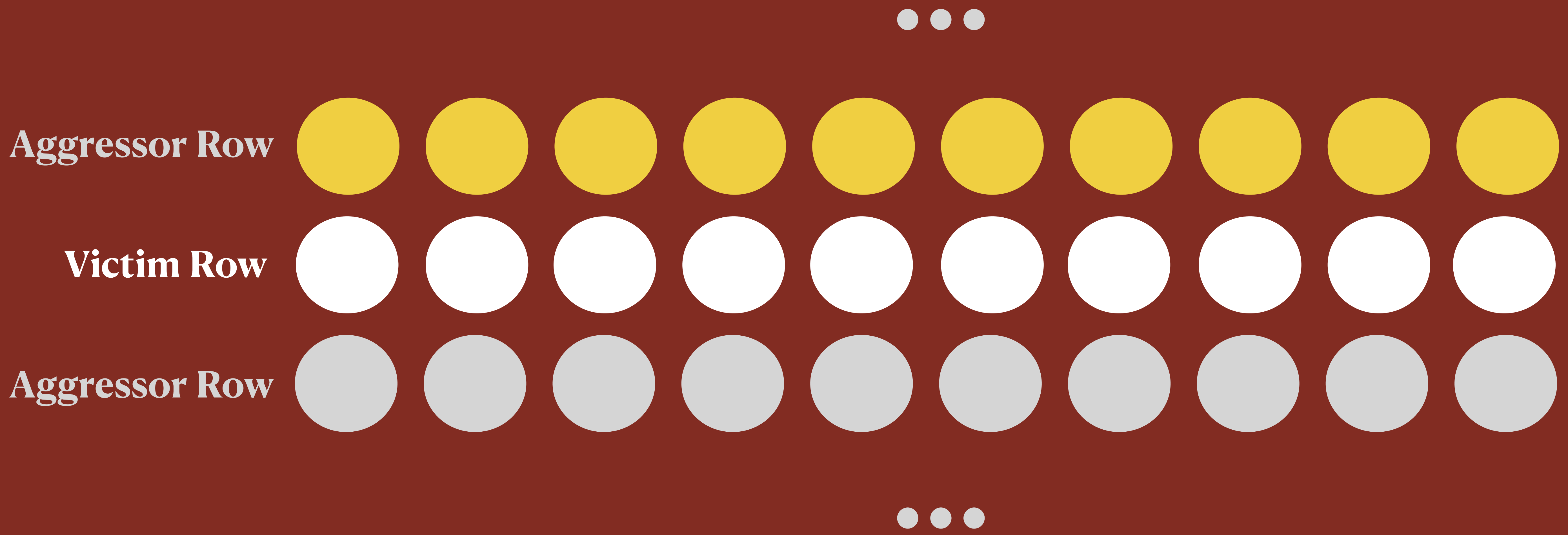


Rowhammer:
Exploit unexpected charge exchange between cells of neighboring rows

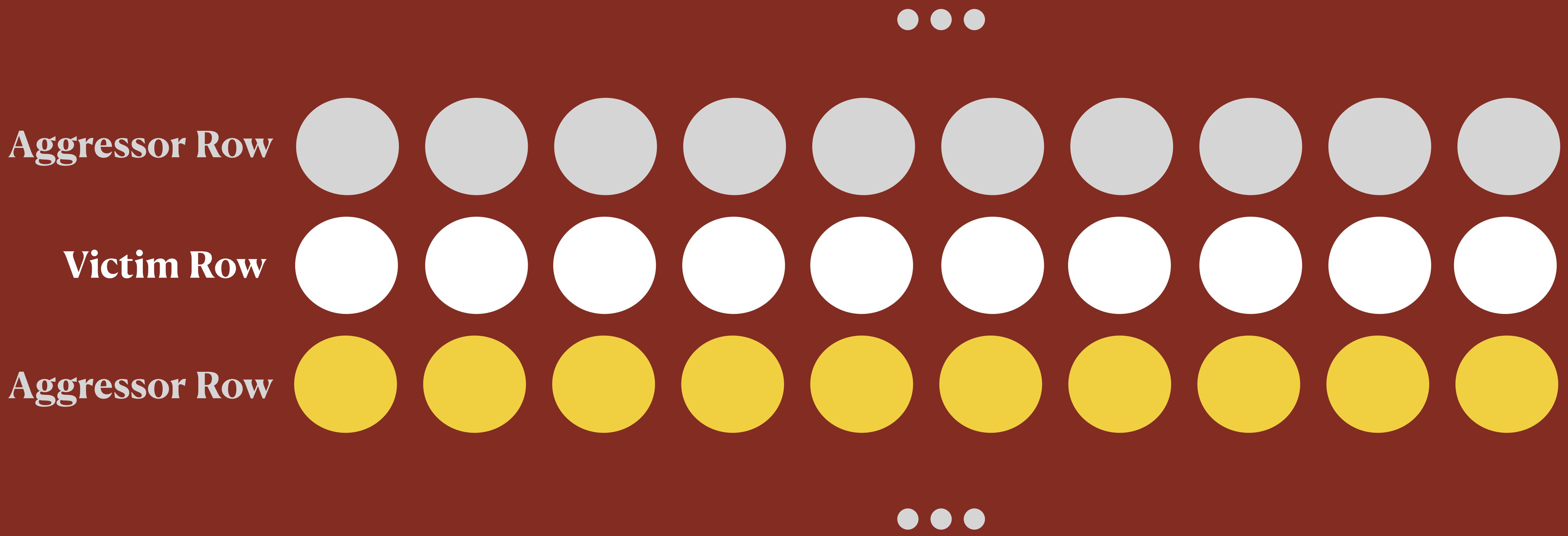
Rowhammer



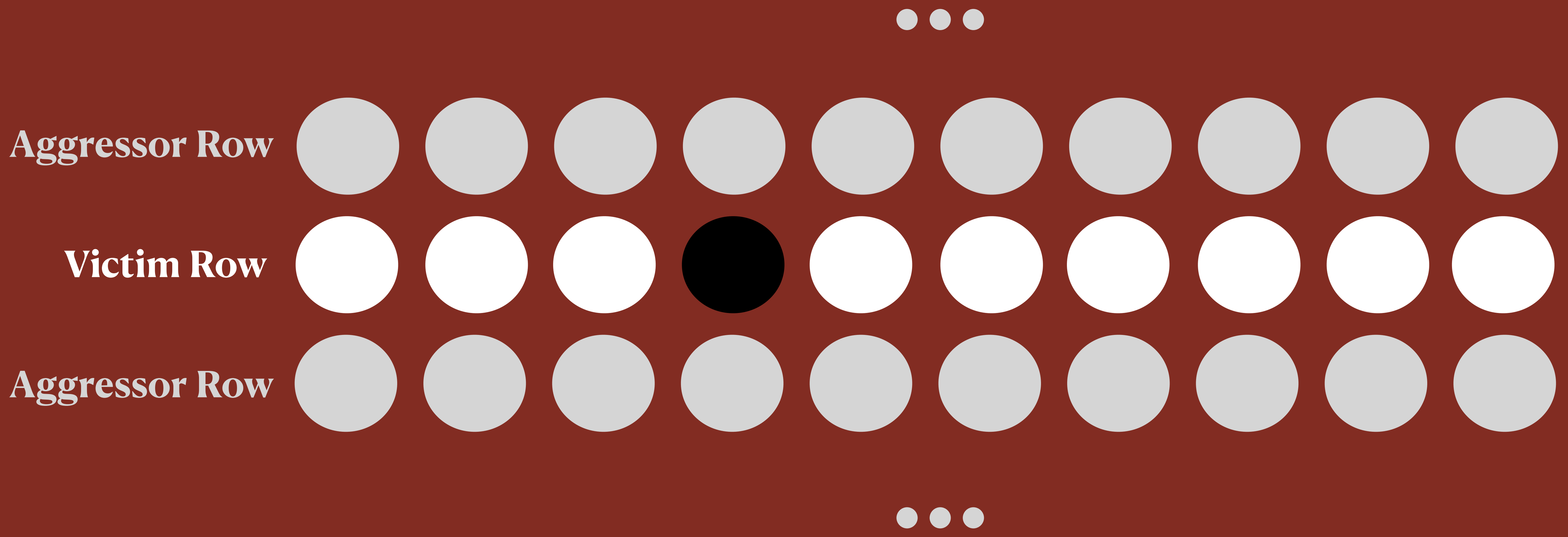
Rowhammer



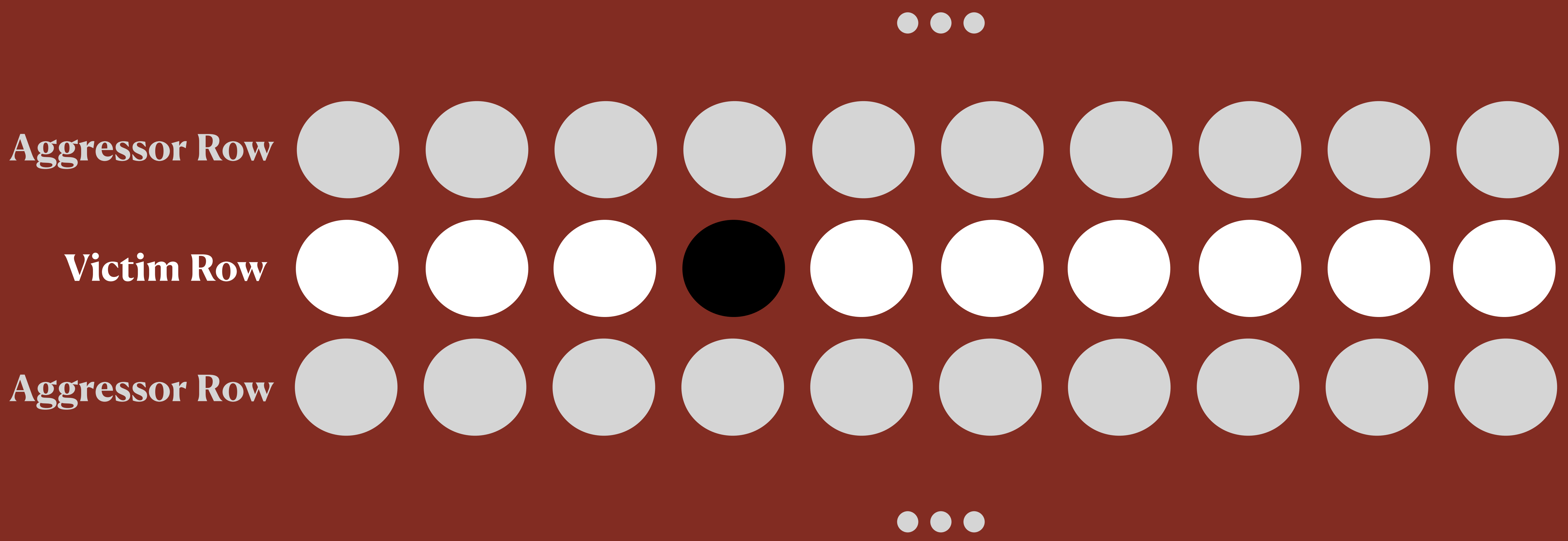
Rowhammer



Rowhammer

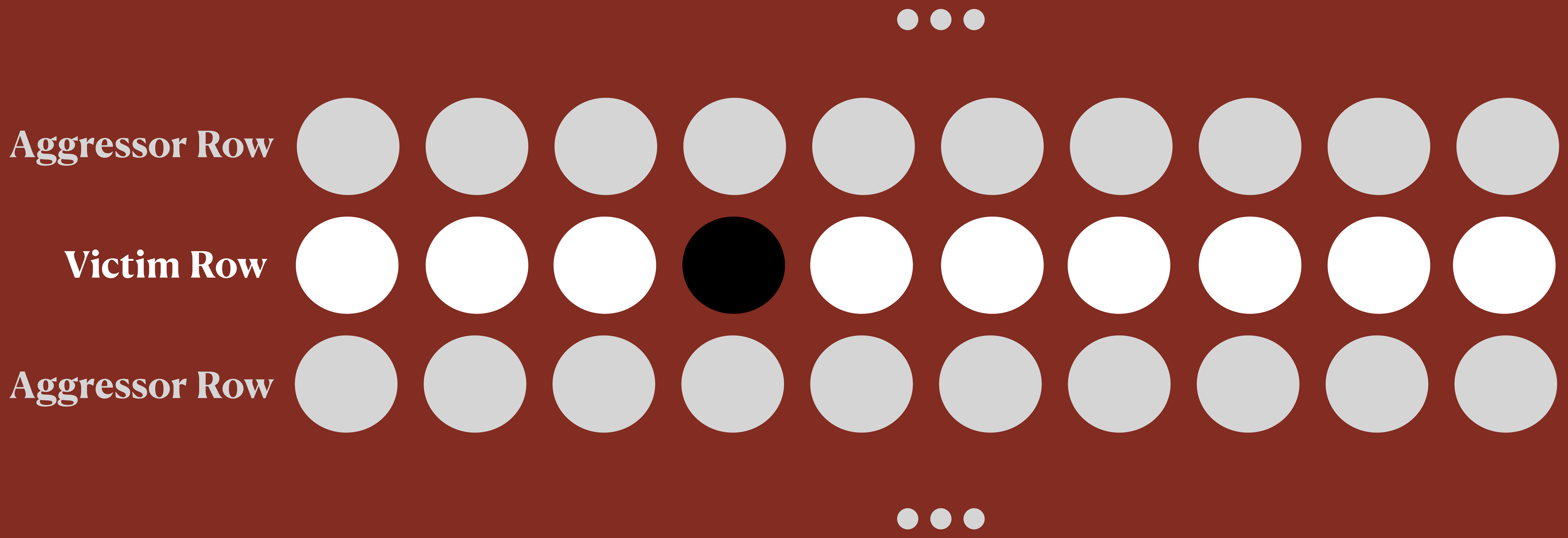


Rowhammer



This bit flip may not be useful...

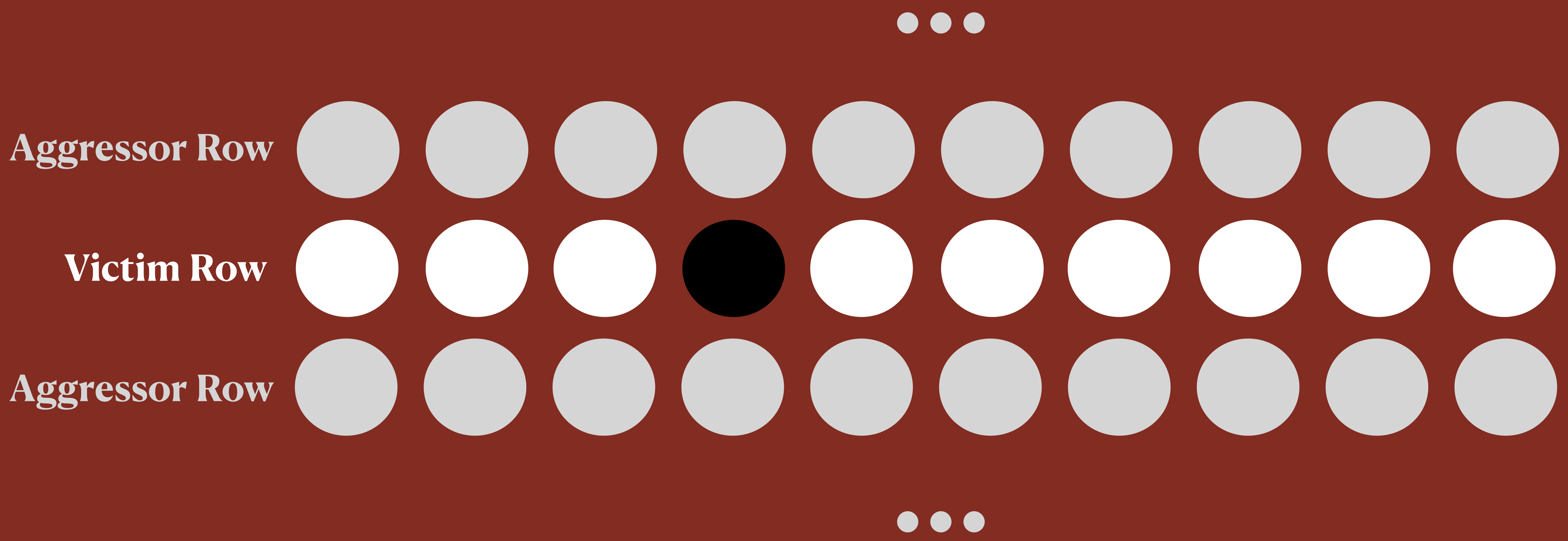
Rowhammer



This bit flip may not be useful...

Repeat?

Rowhammer

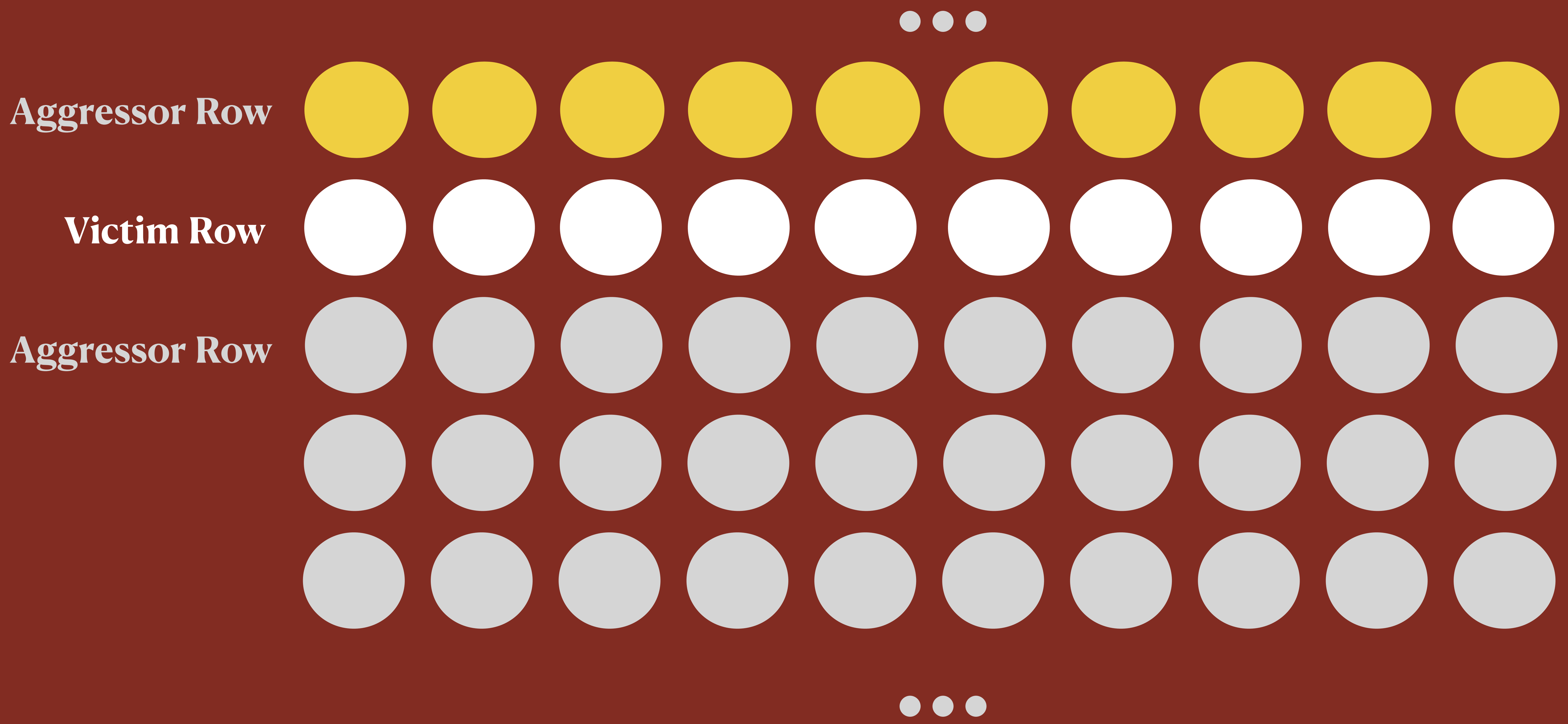


This bit flip may not be useful...

Repeat?

Hammering the same rows gives the same flips!

Templating



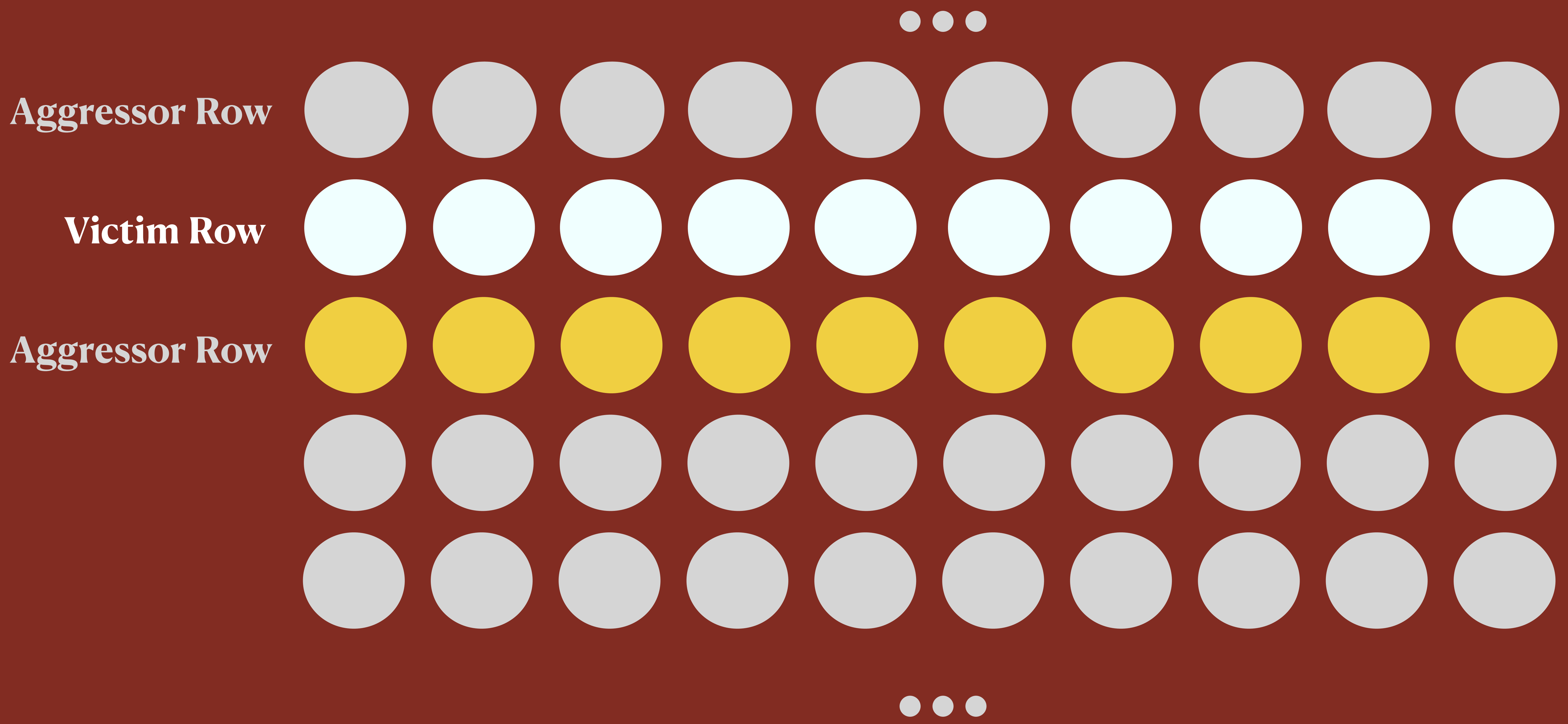
Aggressor Row

Victim Row

Aggressor Row

Row	Cell

Templating



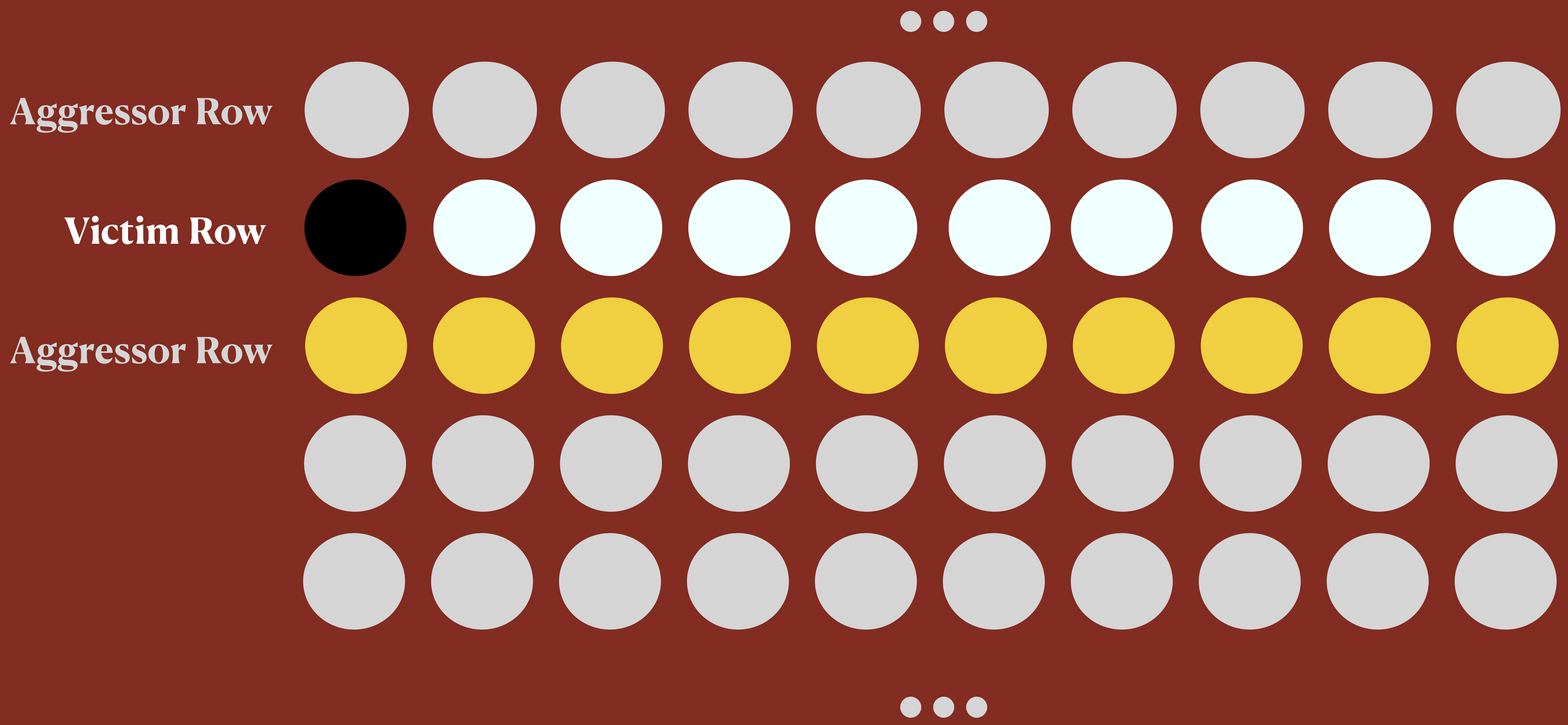
Aggressor Row

Victim Row

Aggressor Row

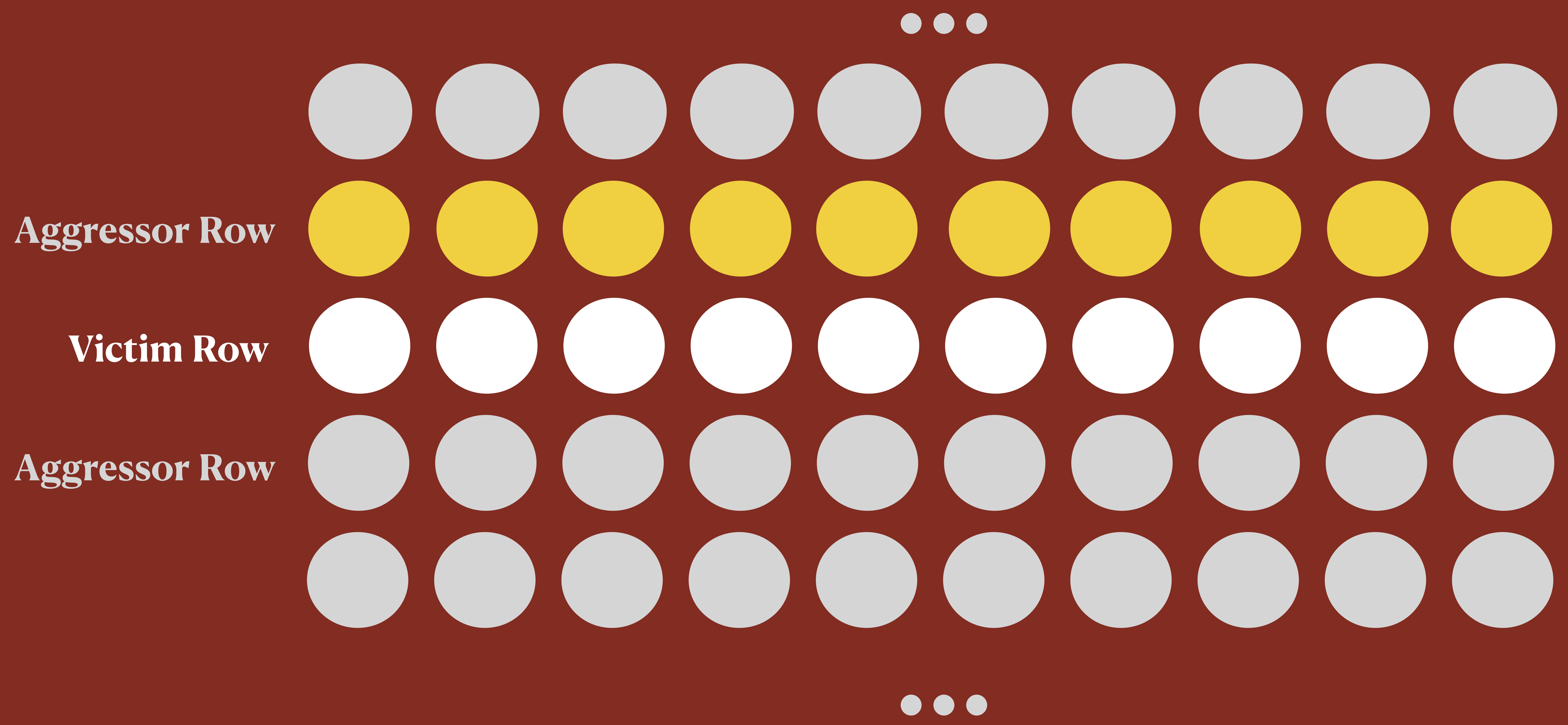
Row	Cell

Templating



Row	Cell
1	0

Templating



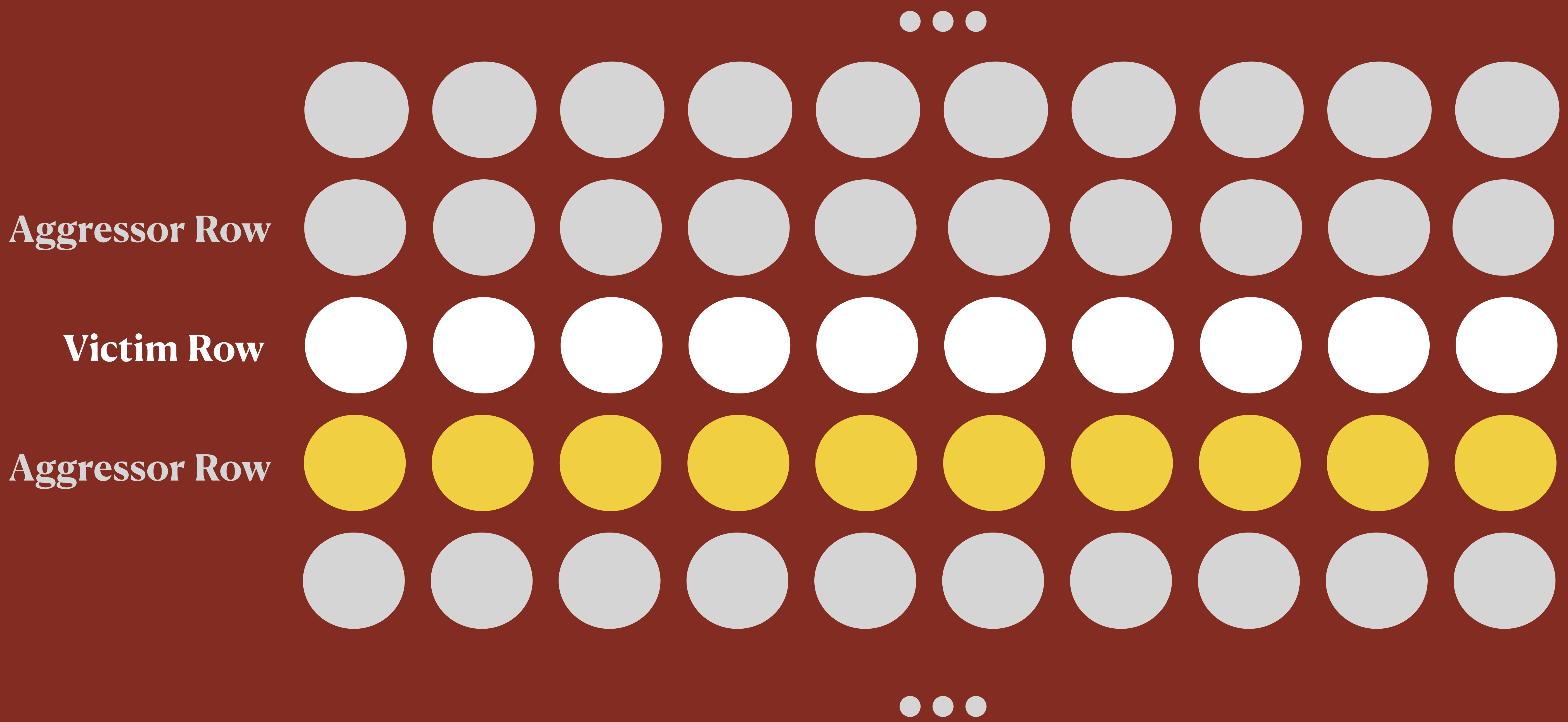
Aggressor Row

Victim Row

Aggressor Row

Row	Cell
1	0

Templating



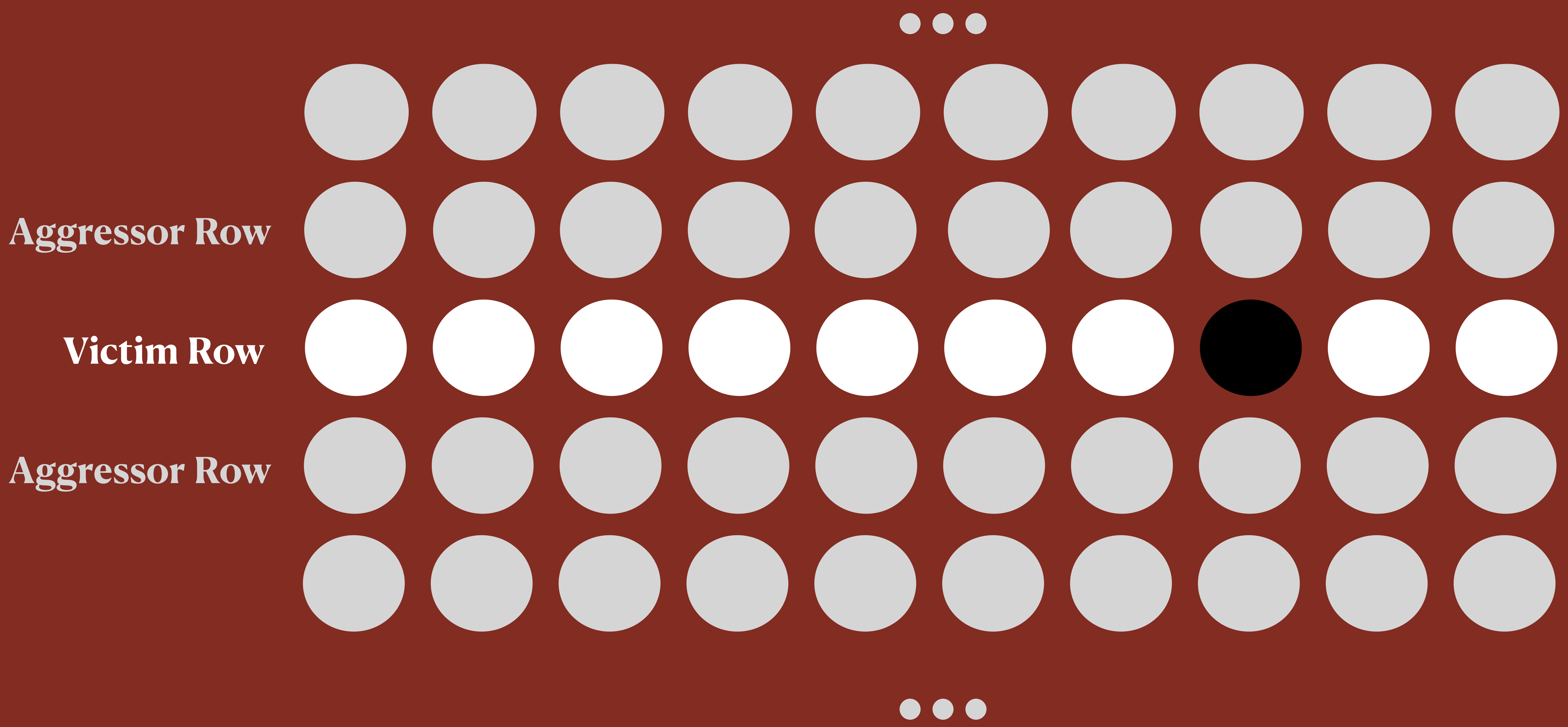
Aggressor Row

Victim Row

Aggressor Row

Row	Cell
1	0

Templating



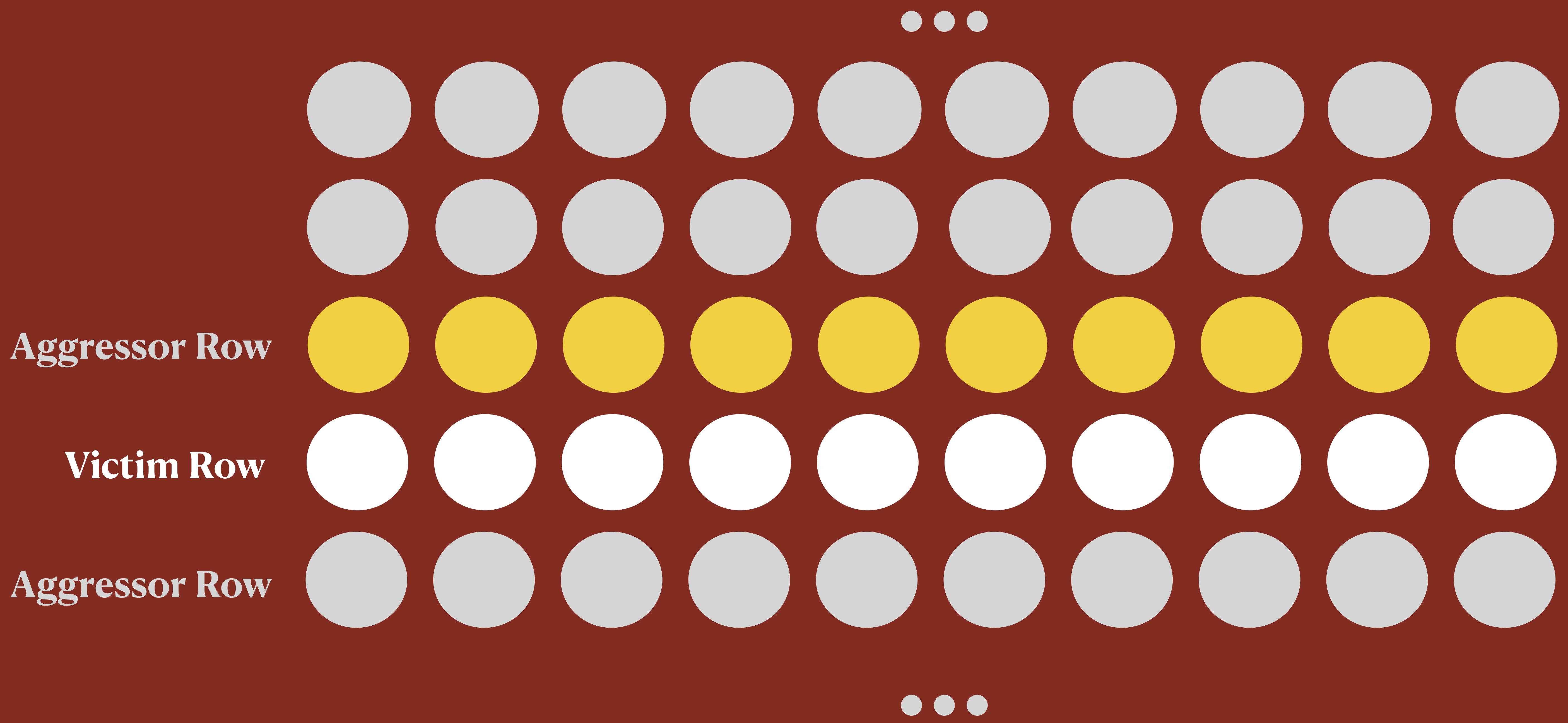
Aggressor Row

Victim Row

Aggressor Row

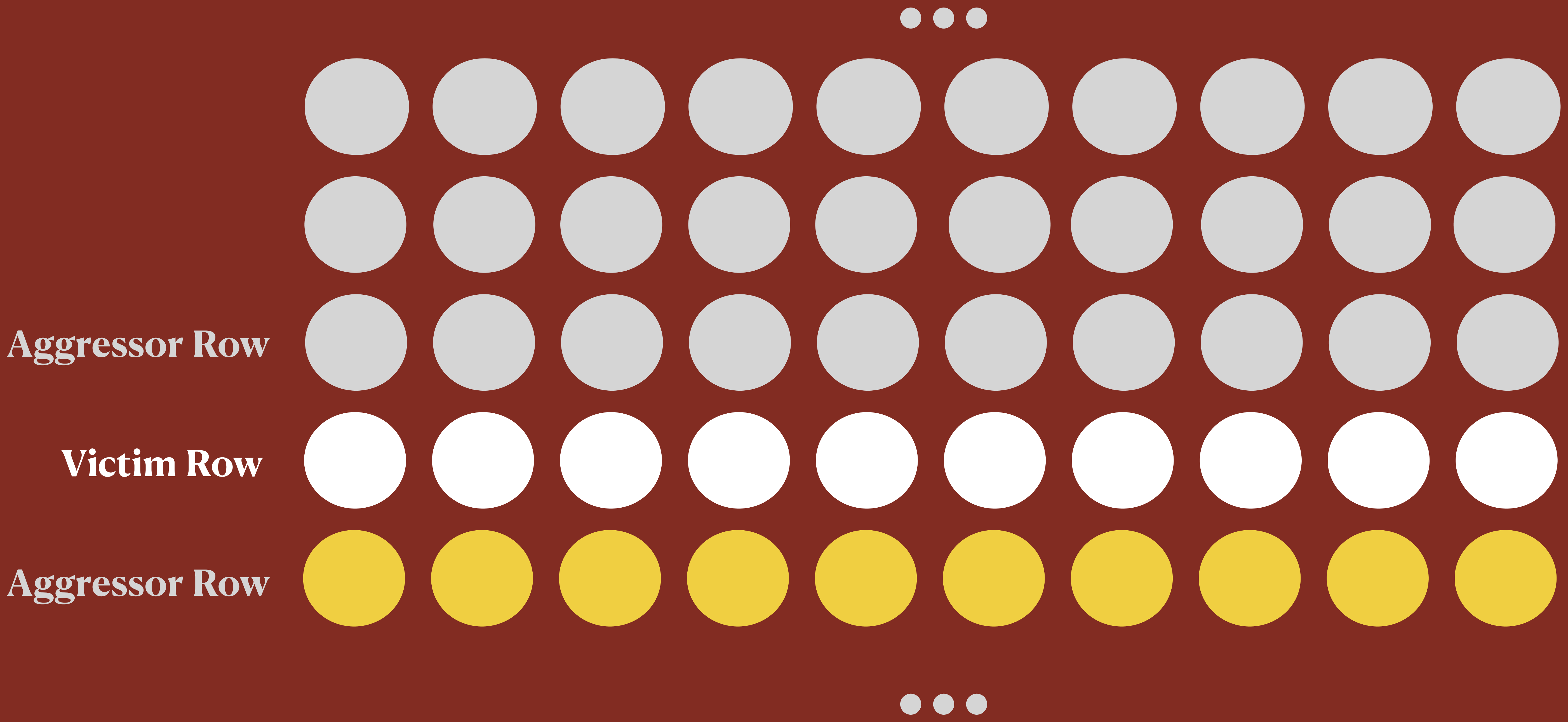
Row	Cell
1	0
2	7

Templating



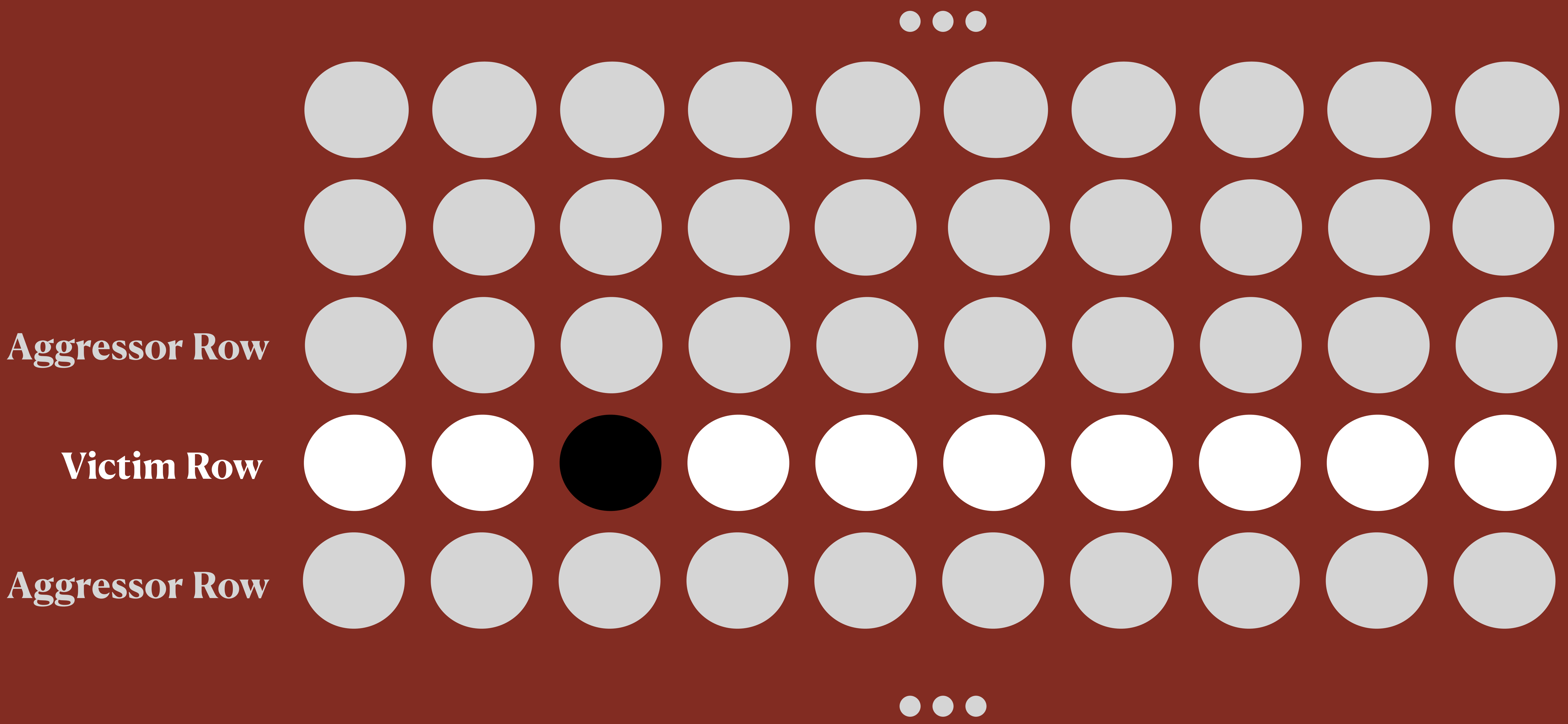
Row	Cell
1	0
2	7

Templating



Row	Cell
1	0
2	7

Templating



Row	Cell
1	0
2	7
3	2

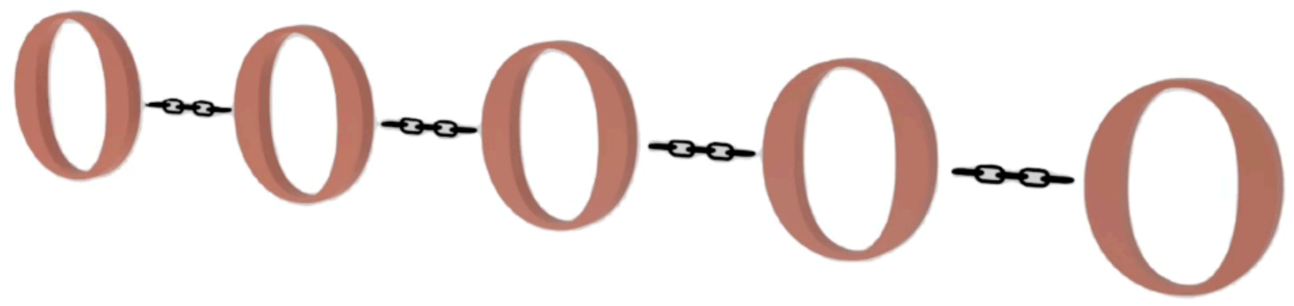
Flip

Simply a bit flip

→ Rowhammer

Feng Shui

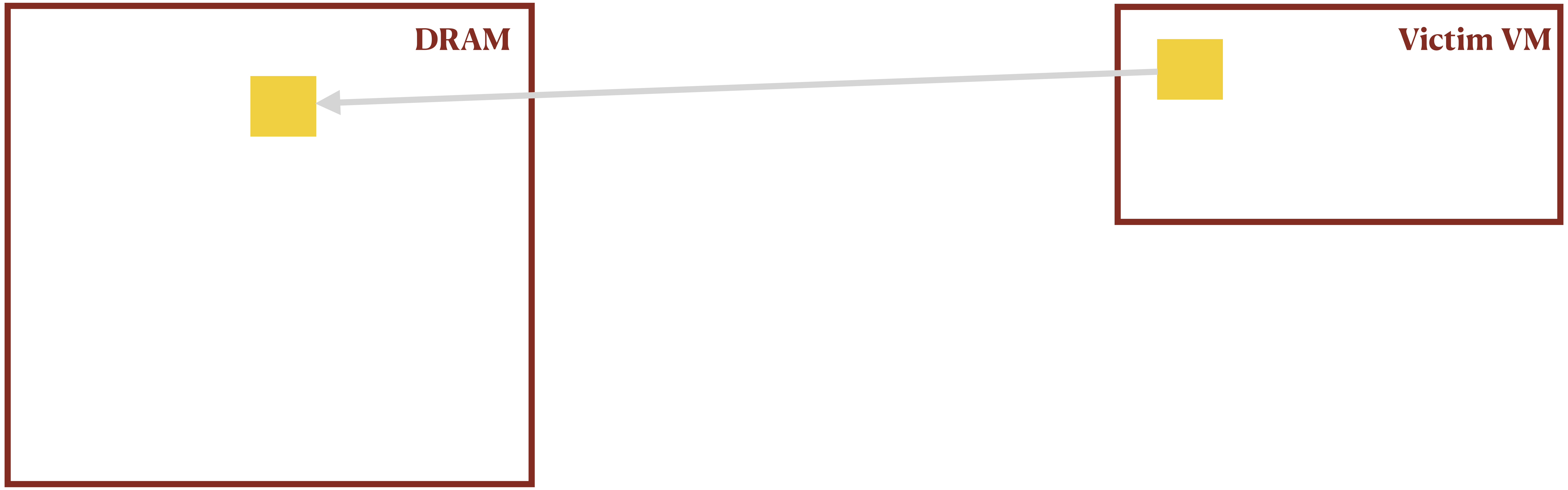
Harmonization with the environment



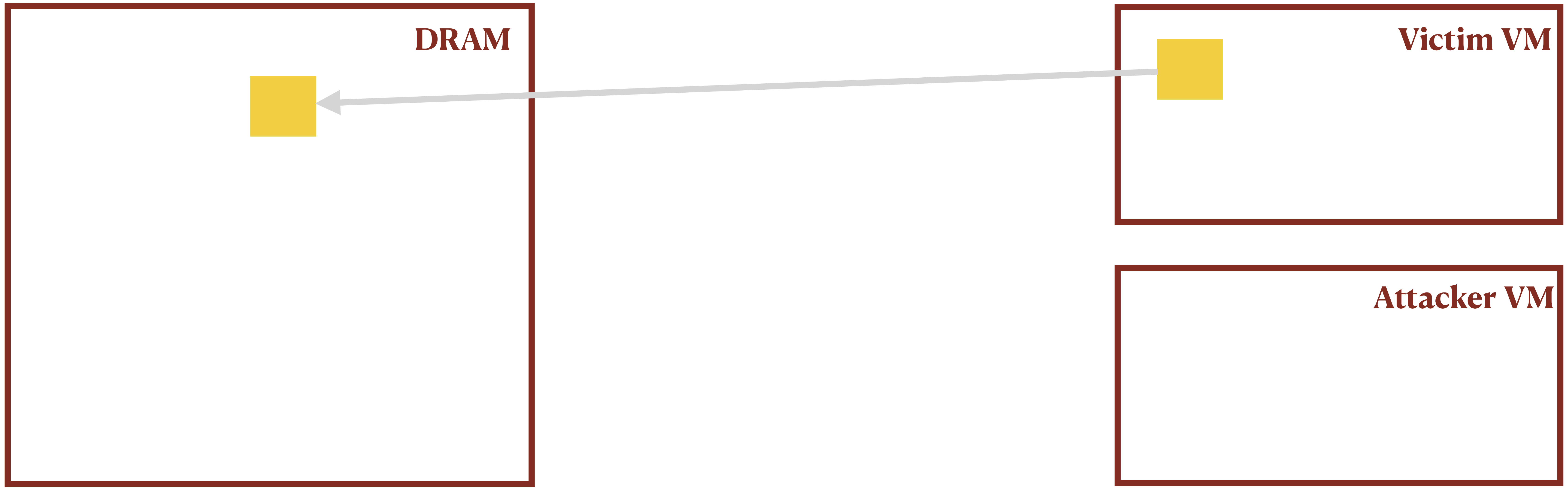
Memory Deduplication

Victim VM

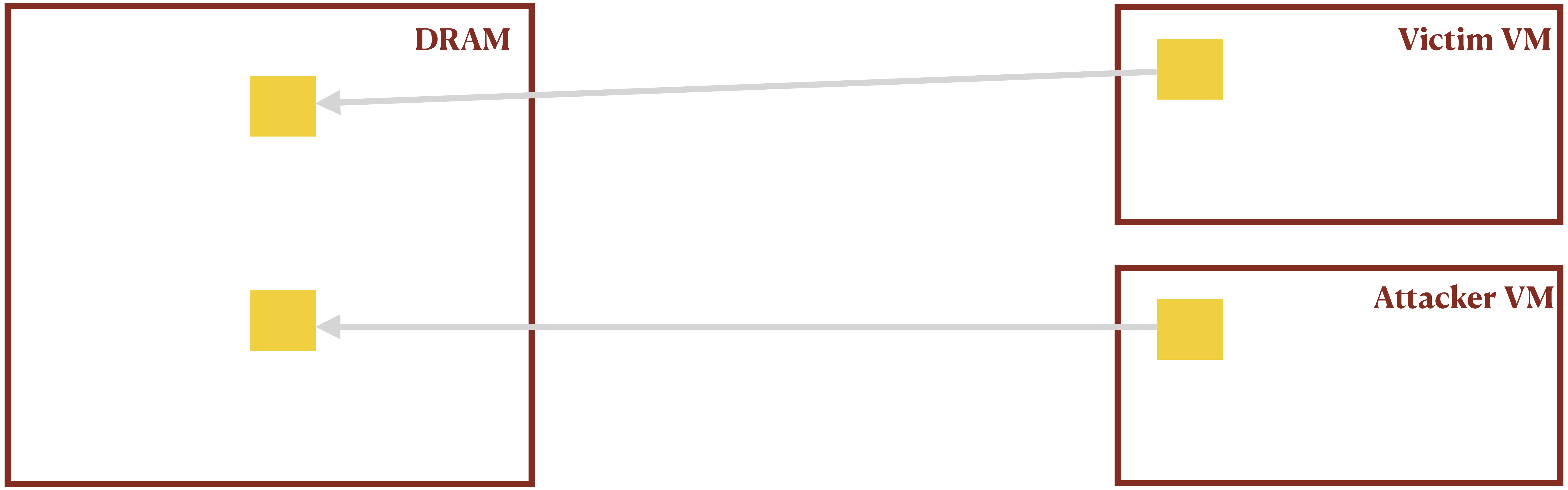
Memory Deduplication



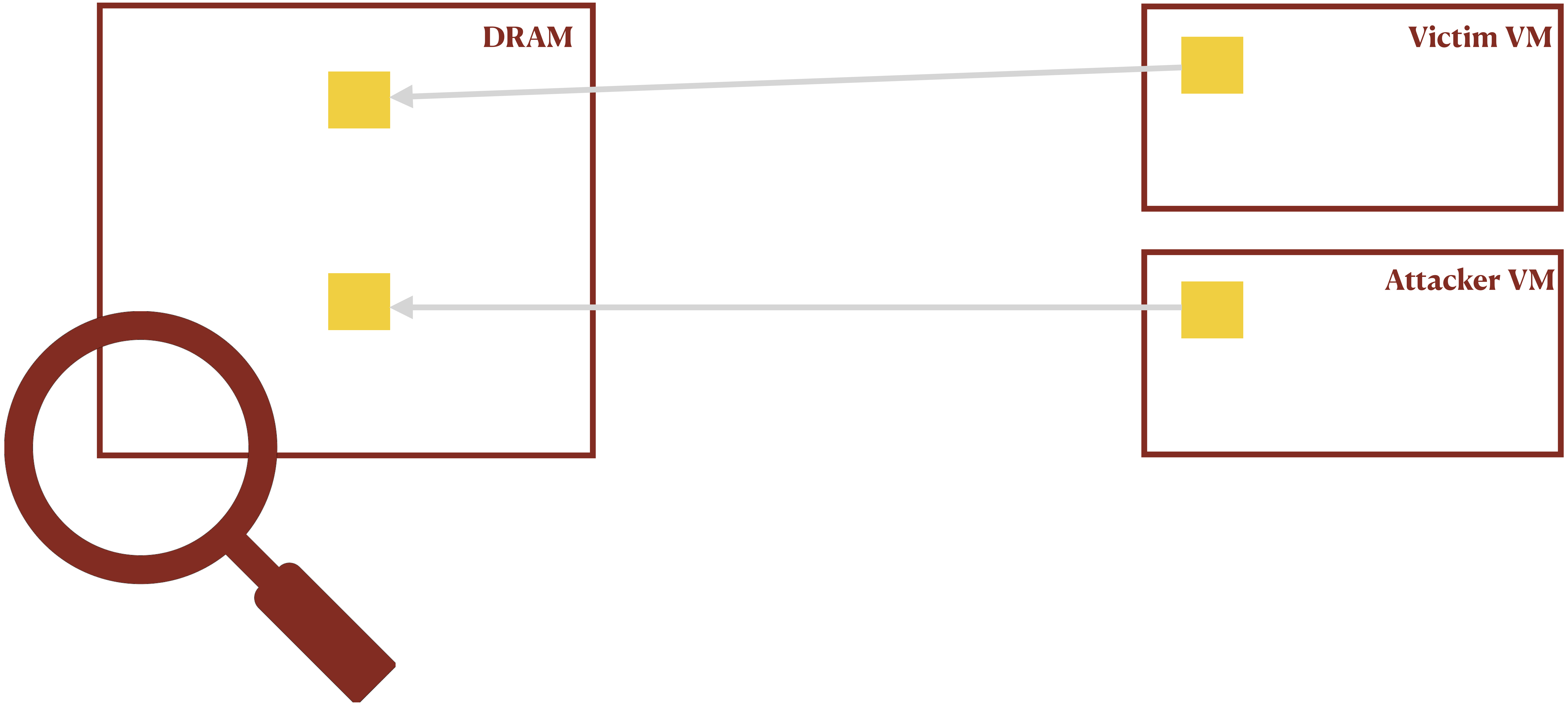
Memory Deduplication



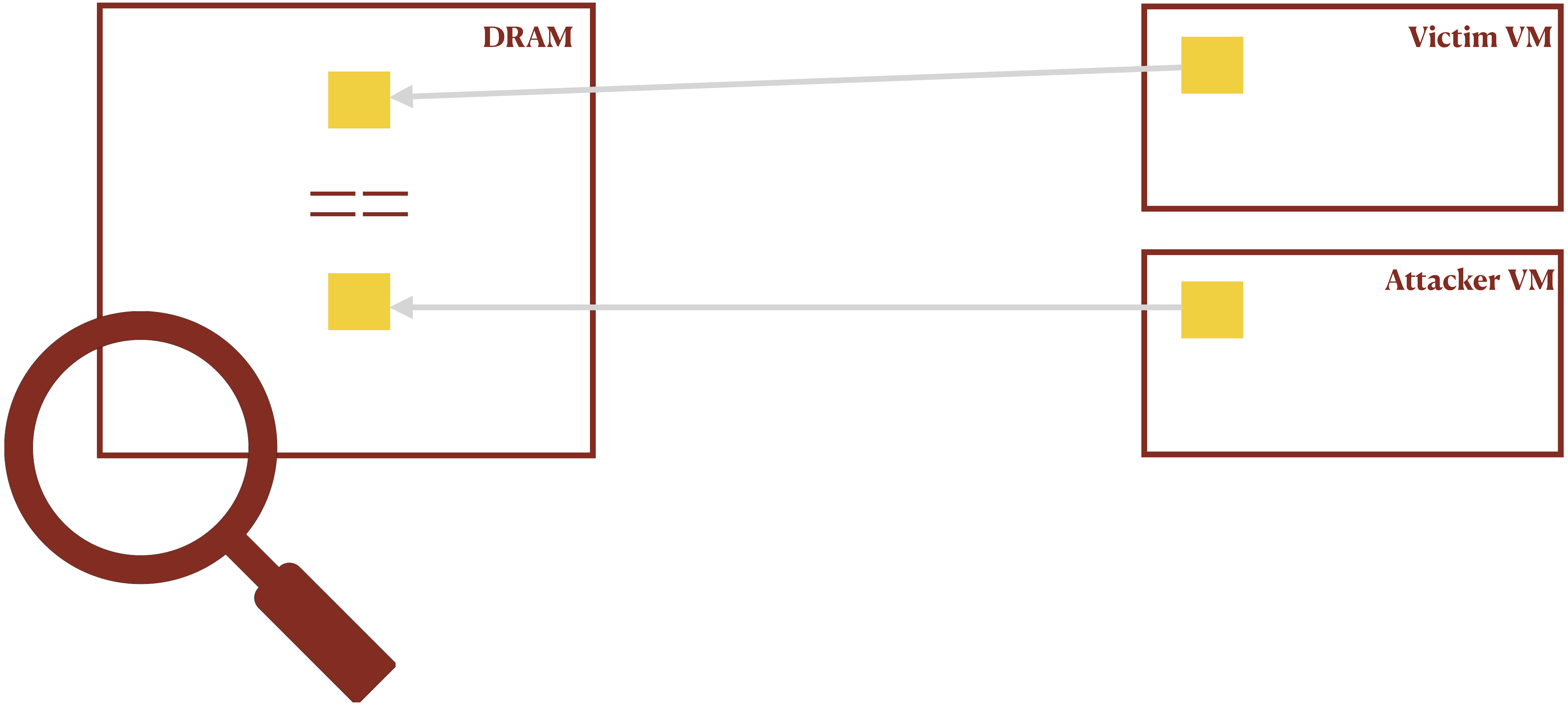
Memory Deduplication



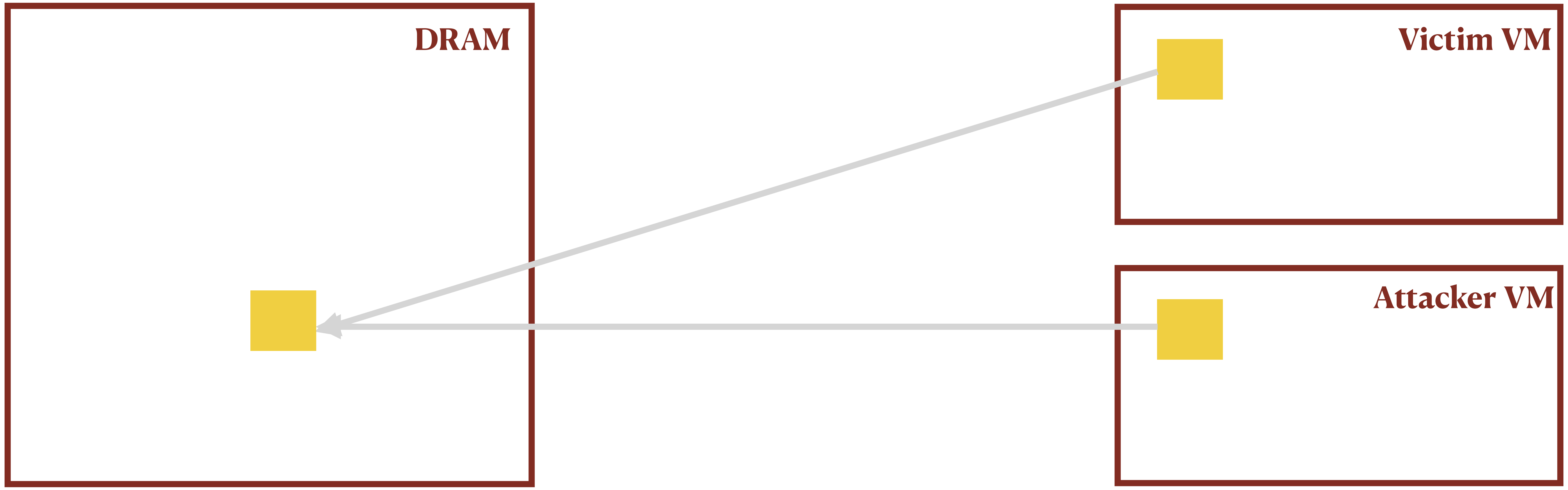
Memory Deduplication



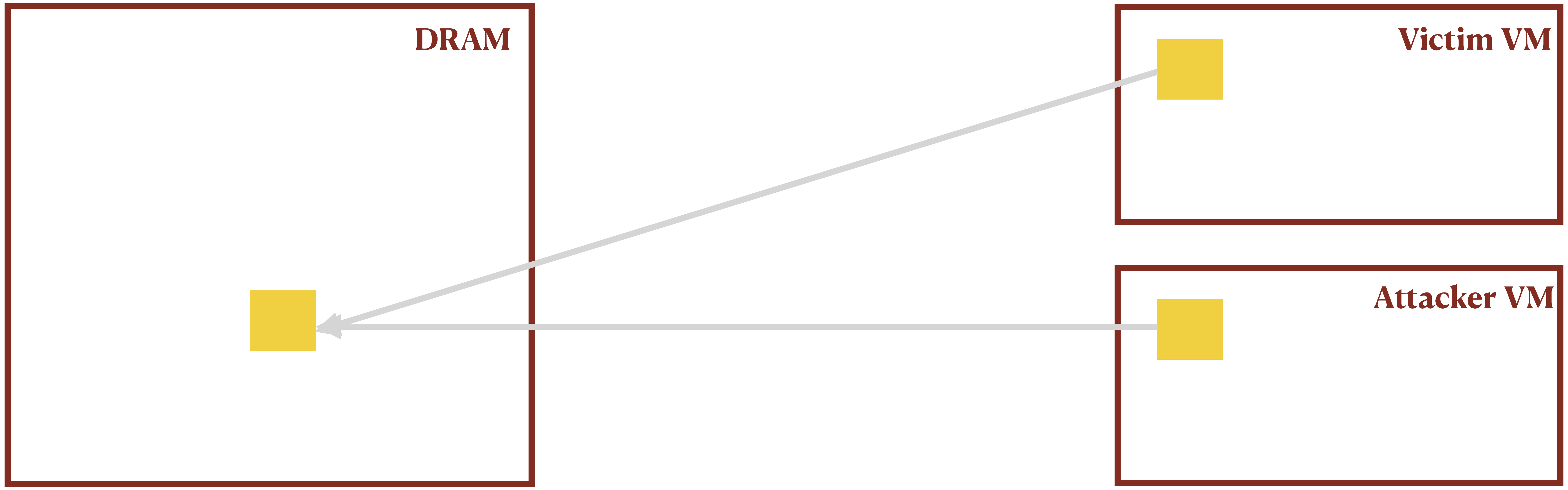
Memory Deduplication



Memory Deduplication



Memory Deduplication



A bit flip in attacker VM ⟷ A bit flip in victim VM

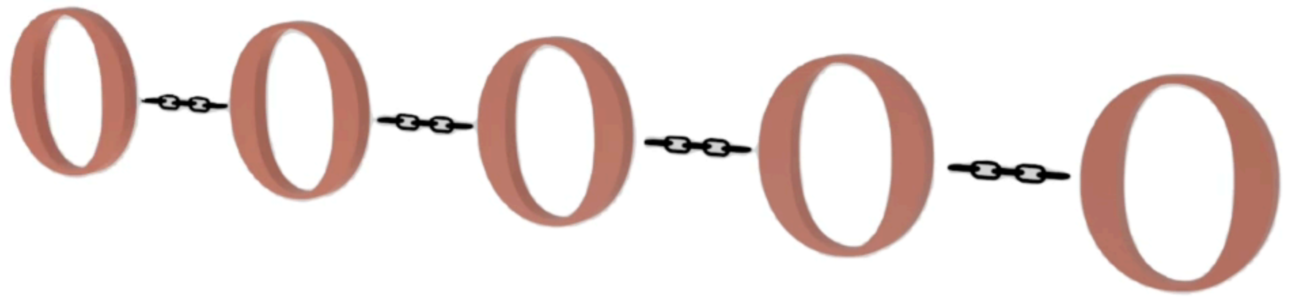
Flip

Simply a bit flip

→ Rowhammer

Feng Shui

Harmonization with the environment



→ Memory dedup.

Using Flip Feng Shui to Attack

- Flip an arbitrary bit in an arbitrary victim page

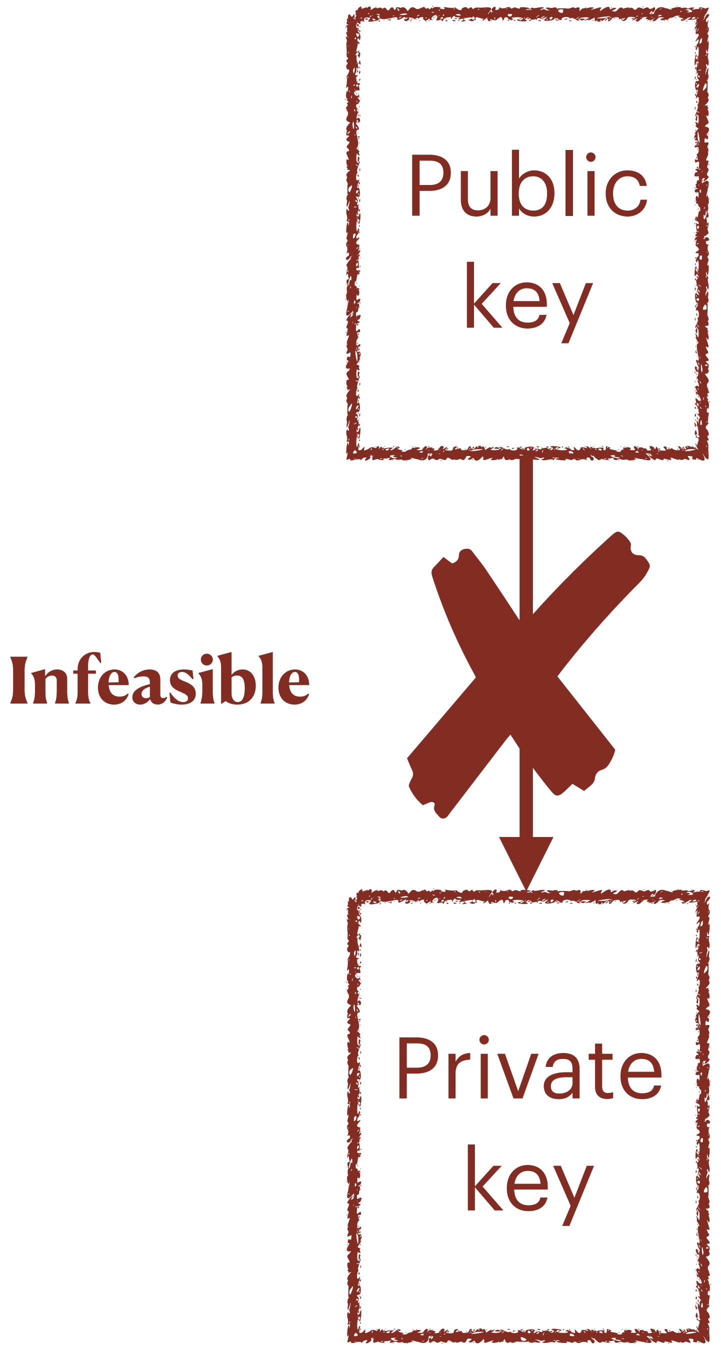
- … that we can know or can predict the contents of

- What is known by an attacker?
  - Public cryptographic information of a victim VM!

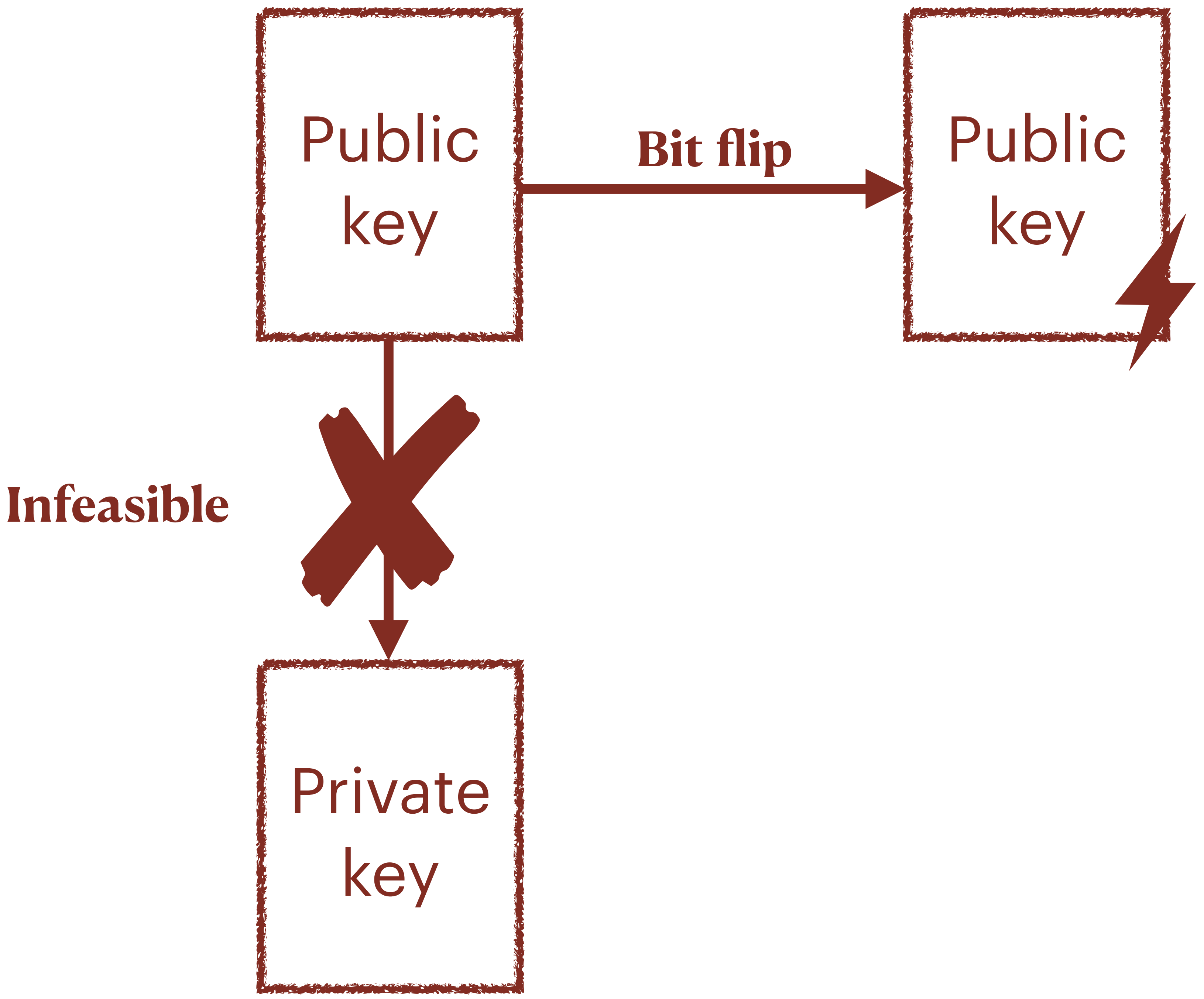
Attacking RSA

Public key

Attacking RSA



Attacking RSA



Public key

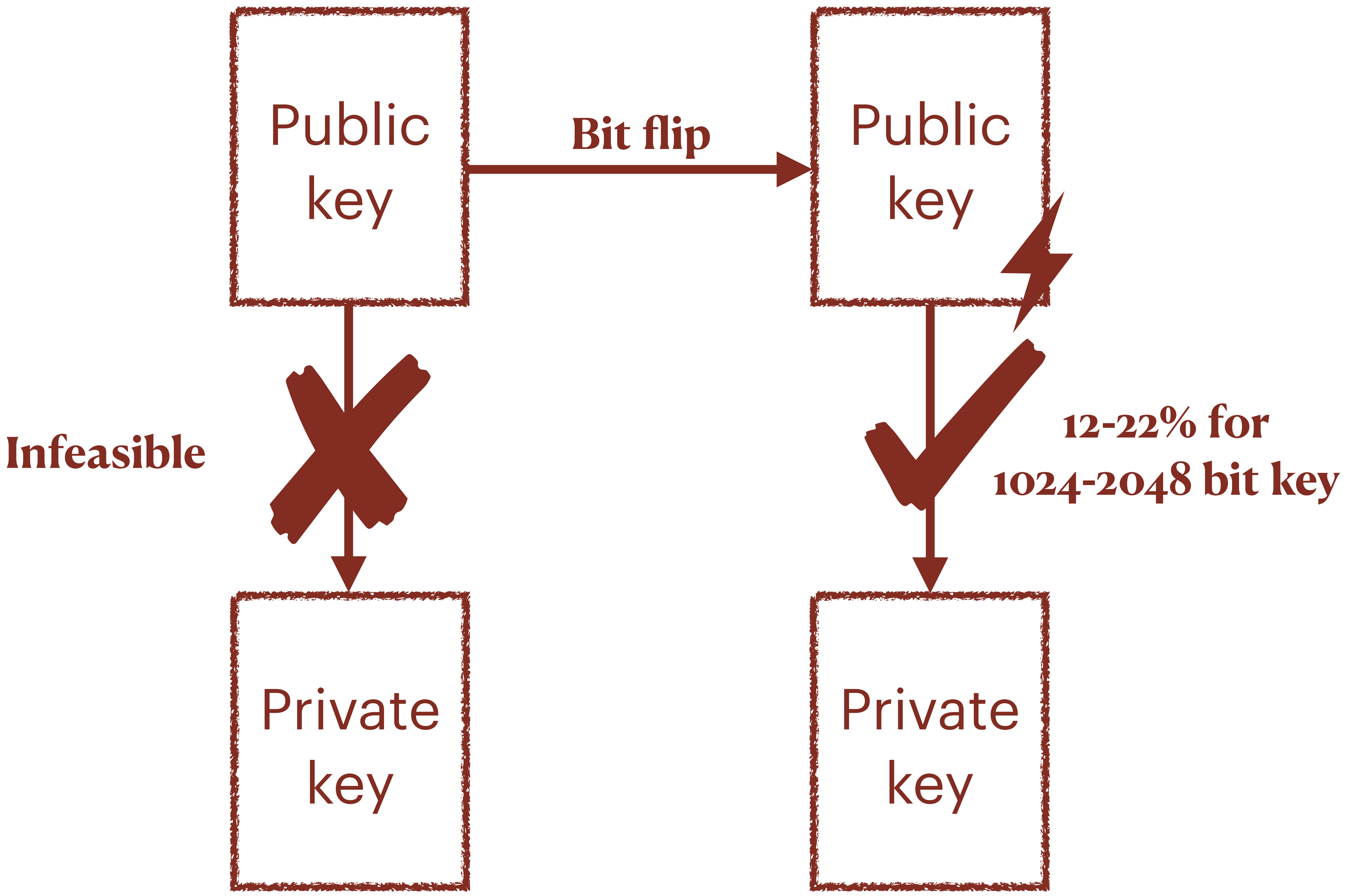
Bit flip

Public key

Infeasible

Private key

Attacking RSA


Public key

Bit flip

Public key

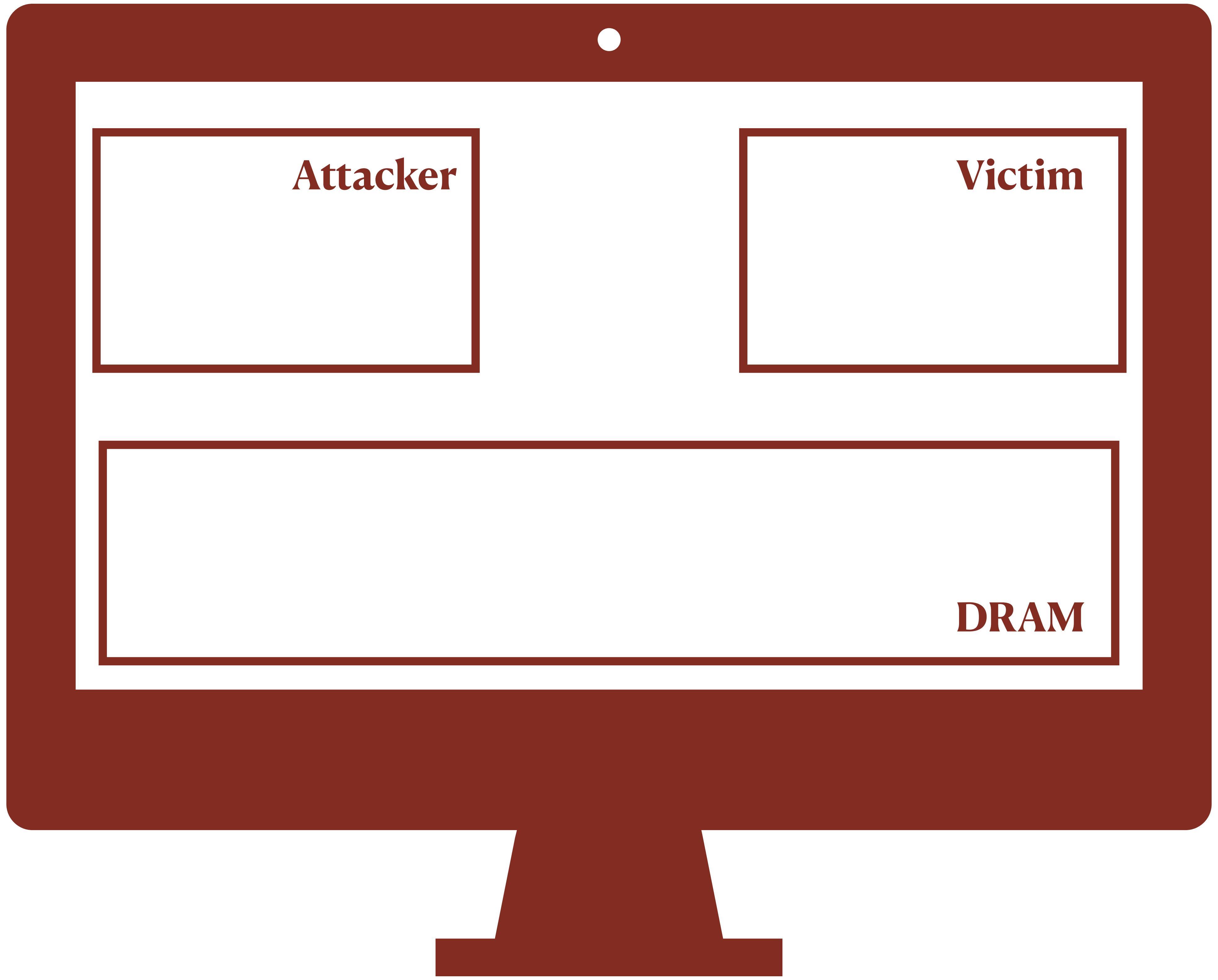
Infeasible

12-22% for 1024-2048 bit key

Private key

Private key

Attack variant: Compromising OpenSSH

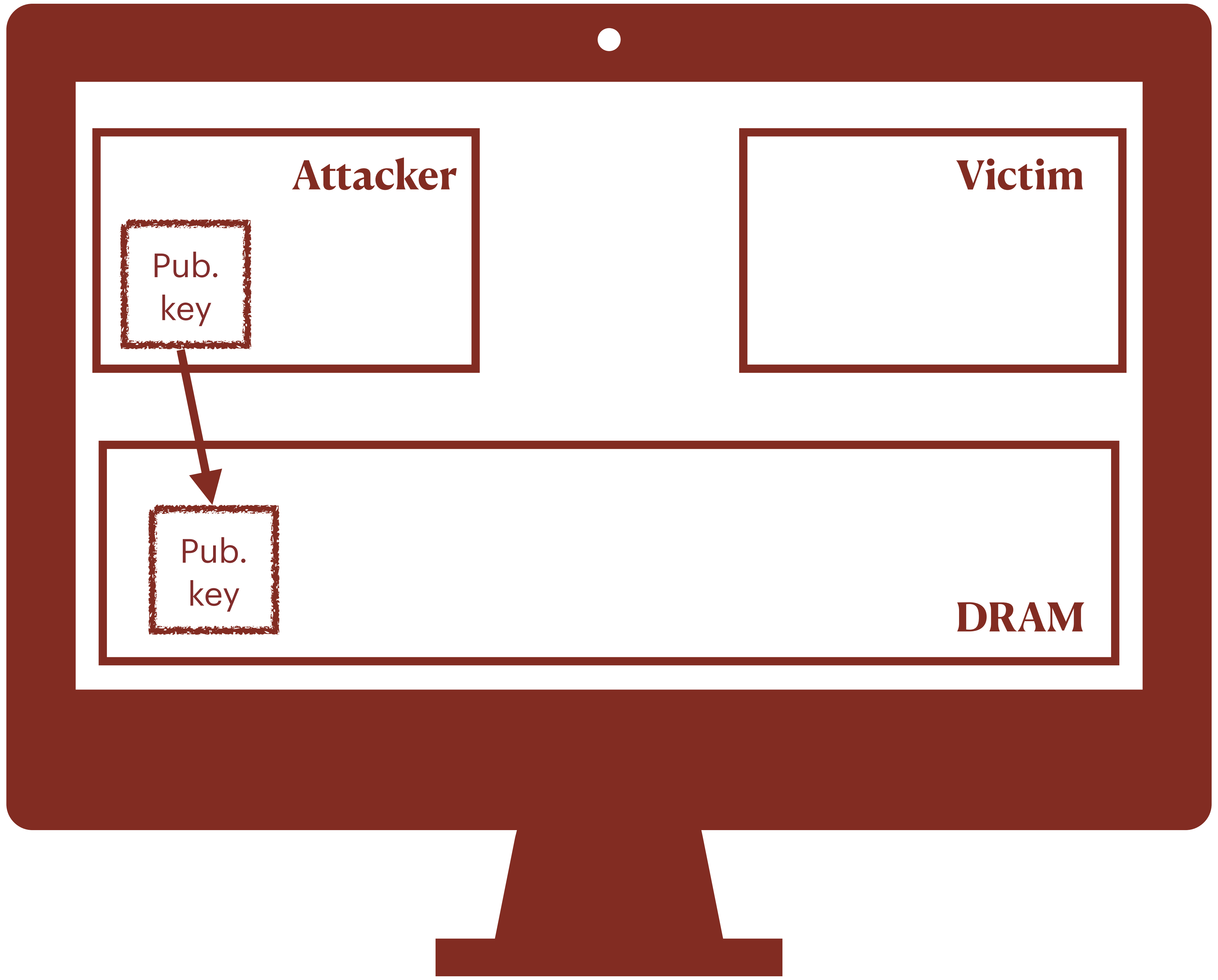


Step 1: Templating

Step 2: Wait for memory deduplication

Step 3: Hammer

Attack variant: Compromising OpenSSH

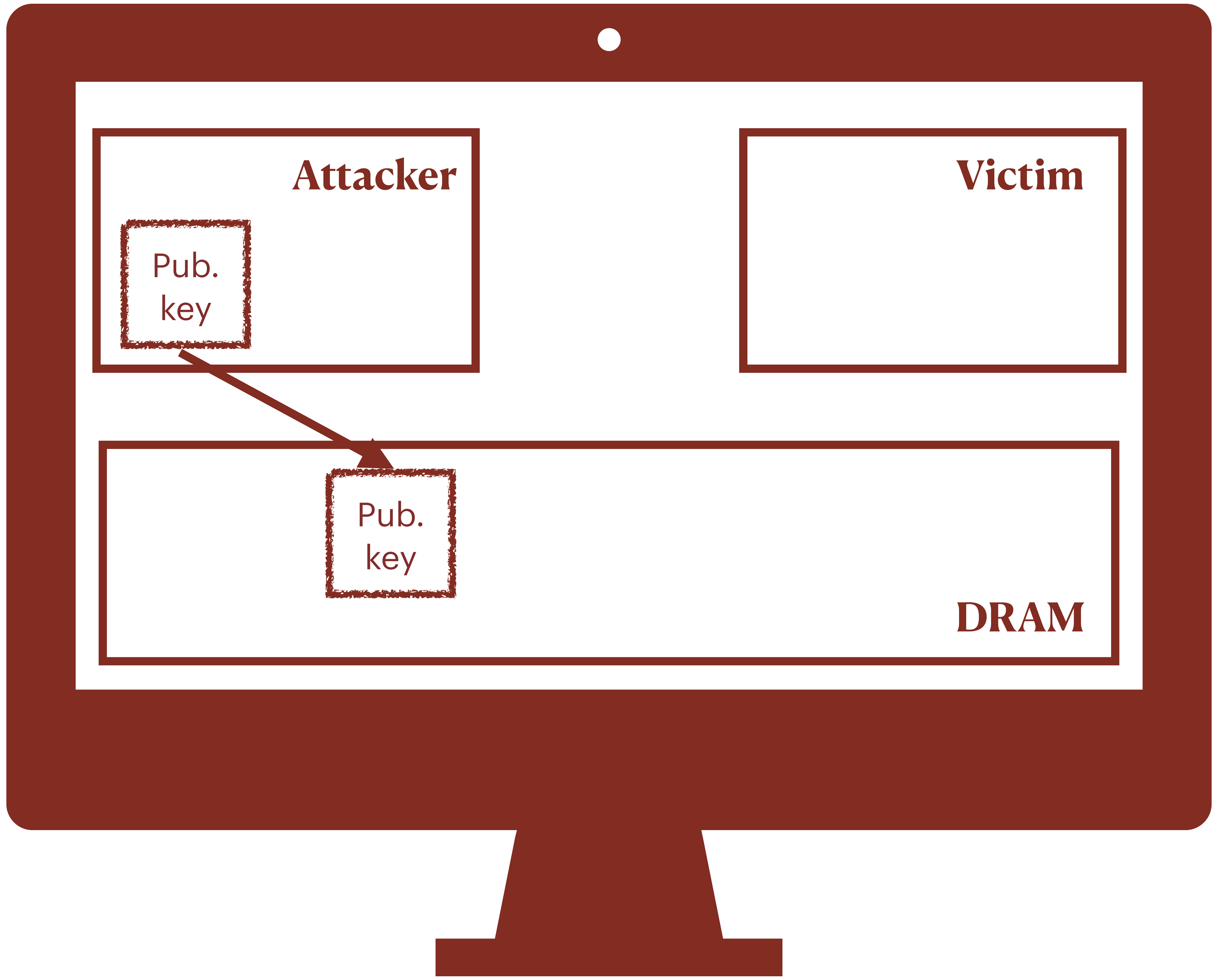


Step 1: Templating

Step 2: Wait for memory deduplication

Step 3: Hammer

Attack variant: Compromising OpenSSH

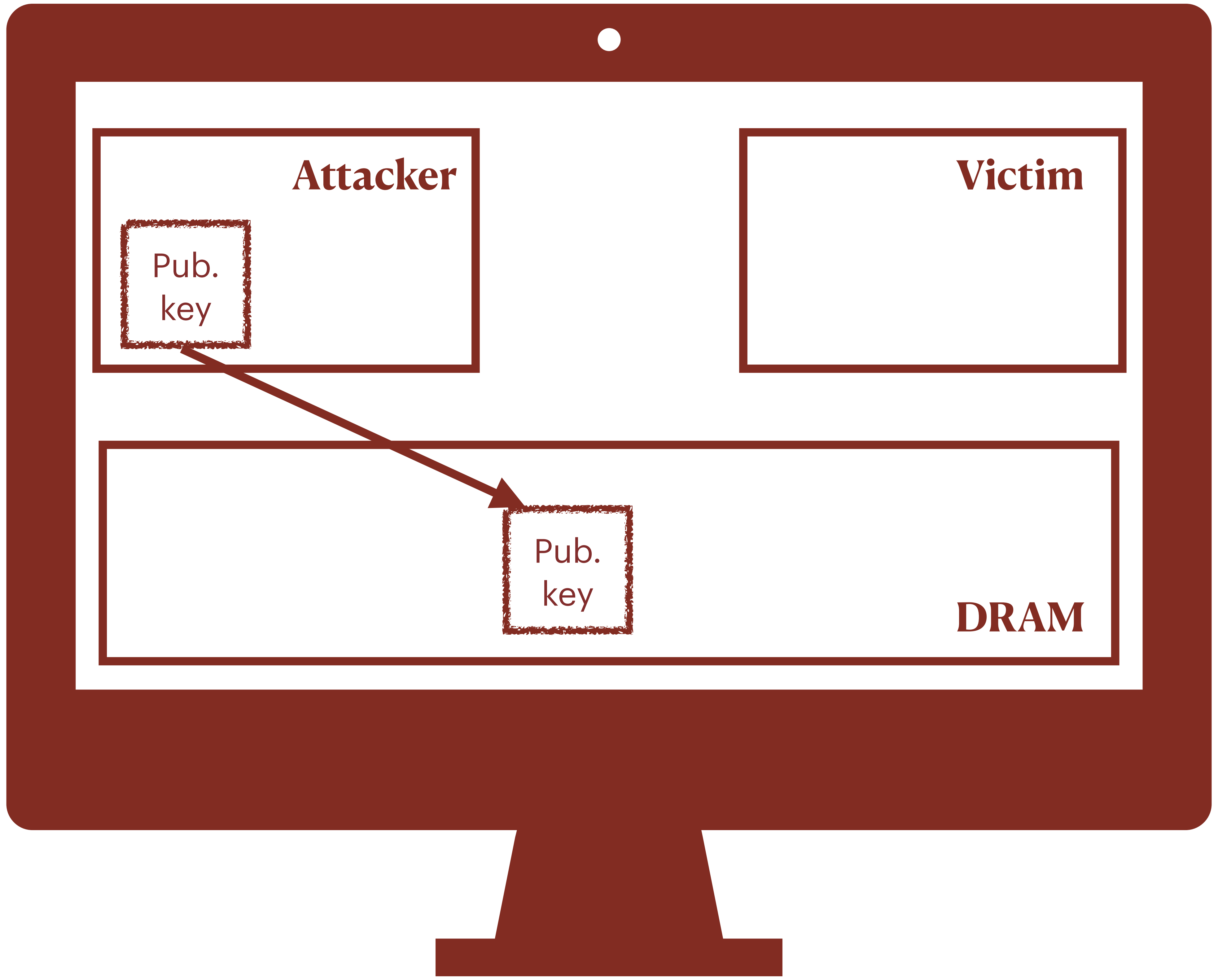


Step 1: Templating

Step 2: Wait for memory deduplication

Step 3: Hammer

Attack variant: Compromising OpenSSH

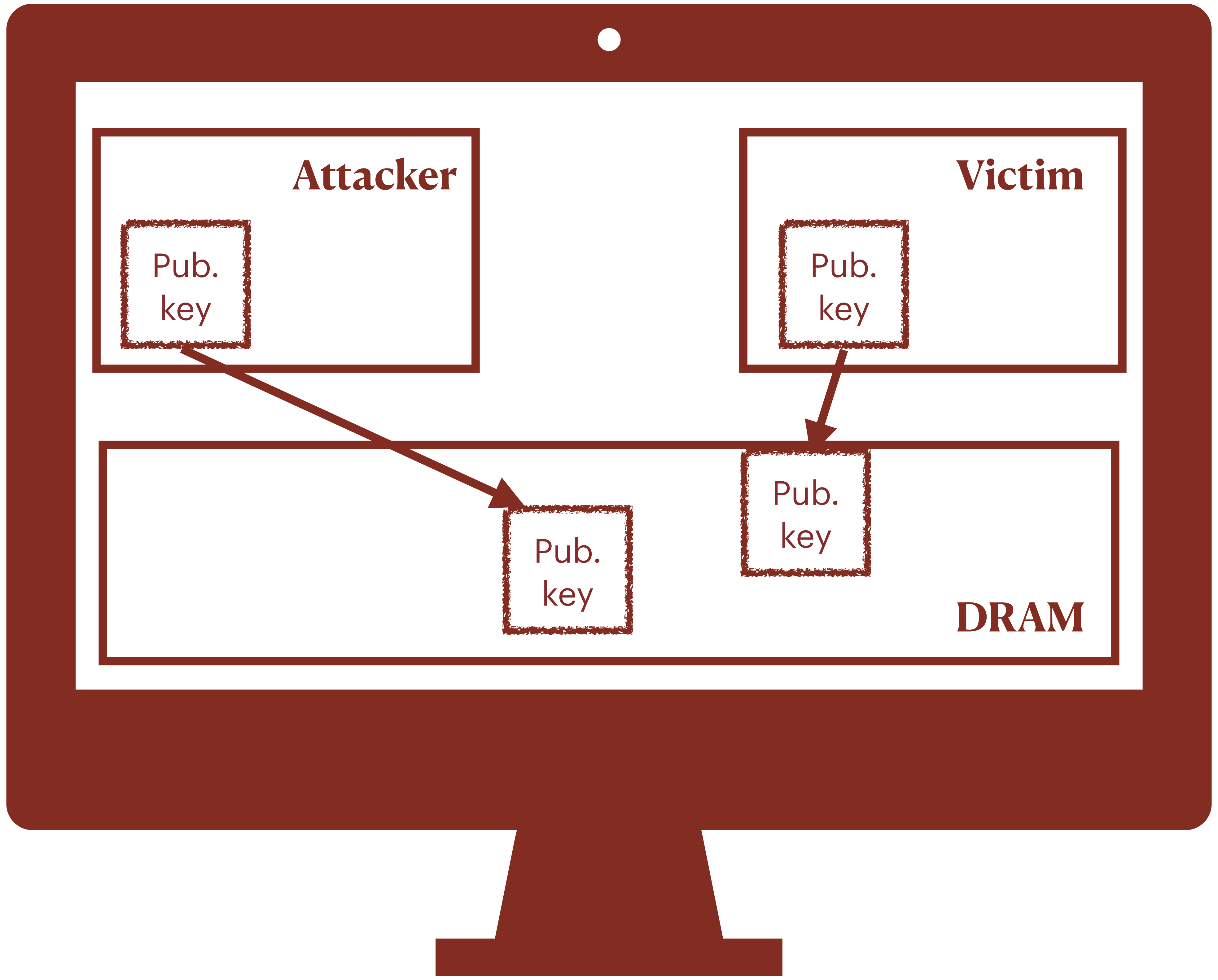


Step 1: Templating

Step 2: Wait for memory deduplication

Step 3: Hammer

Attack variant: Compromising OpenSSH

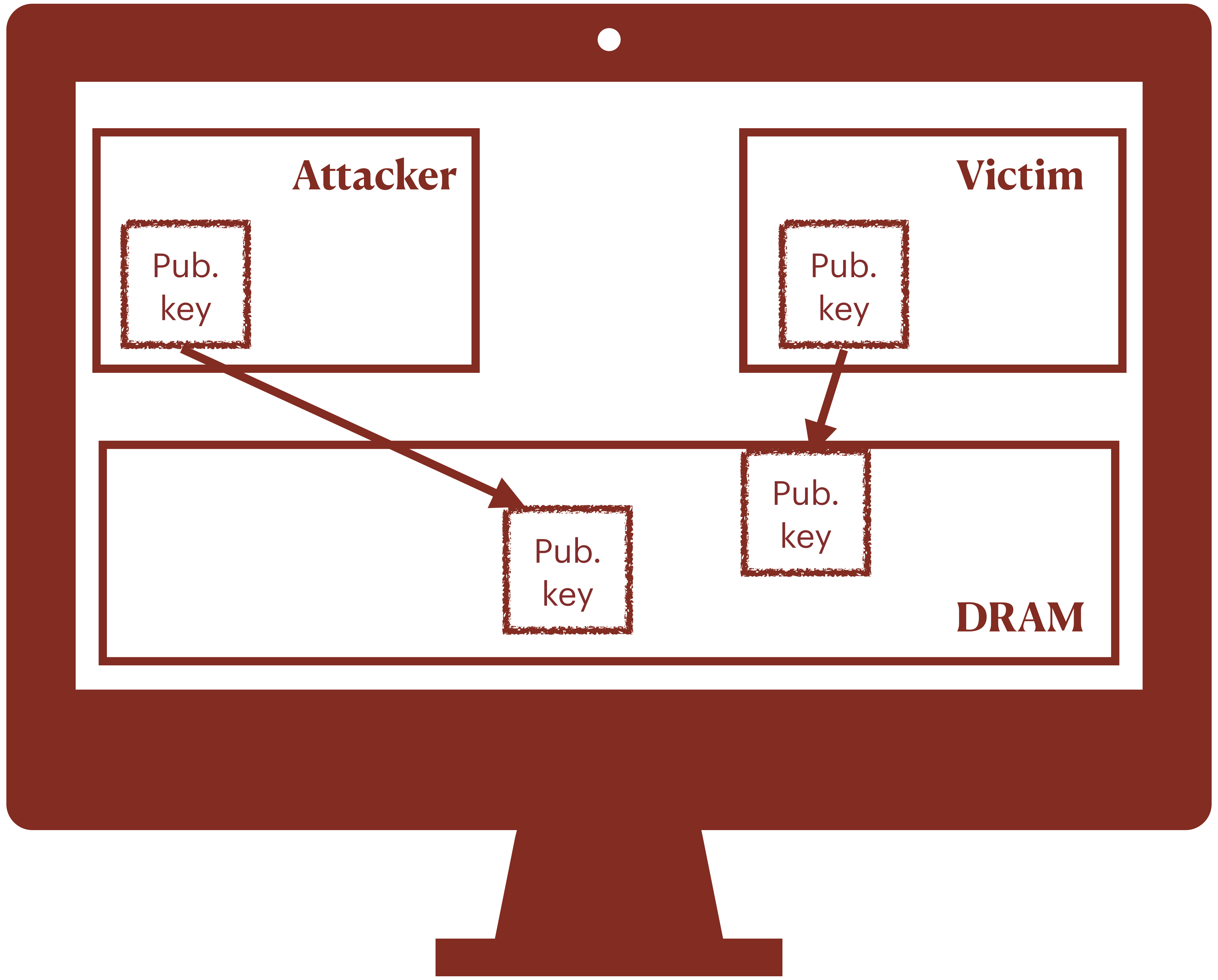


Step 1: Templating

Step 2: Wait for memory deduplication

Step 3: Hammer

Attack variant: Compromising OpenSSH

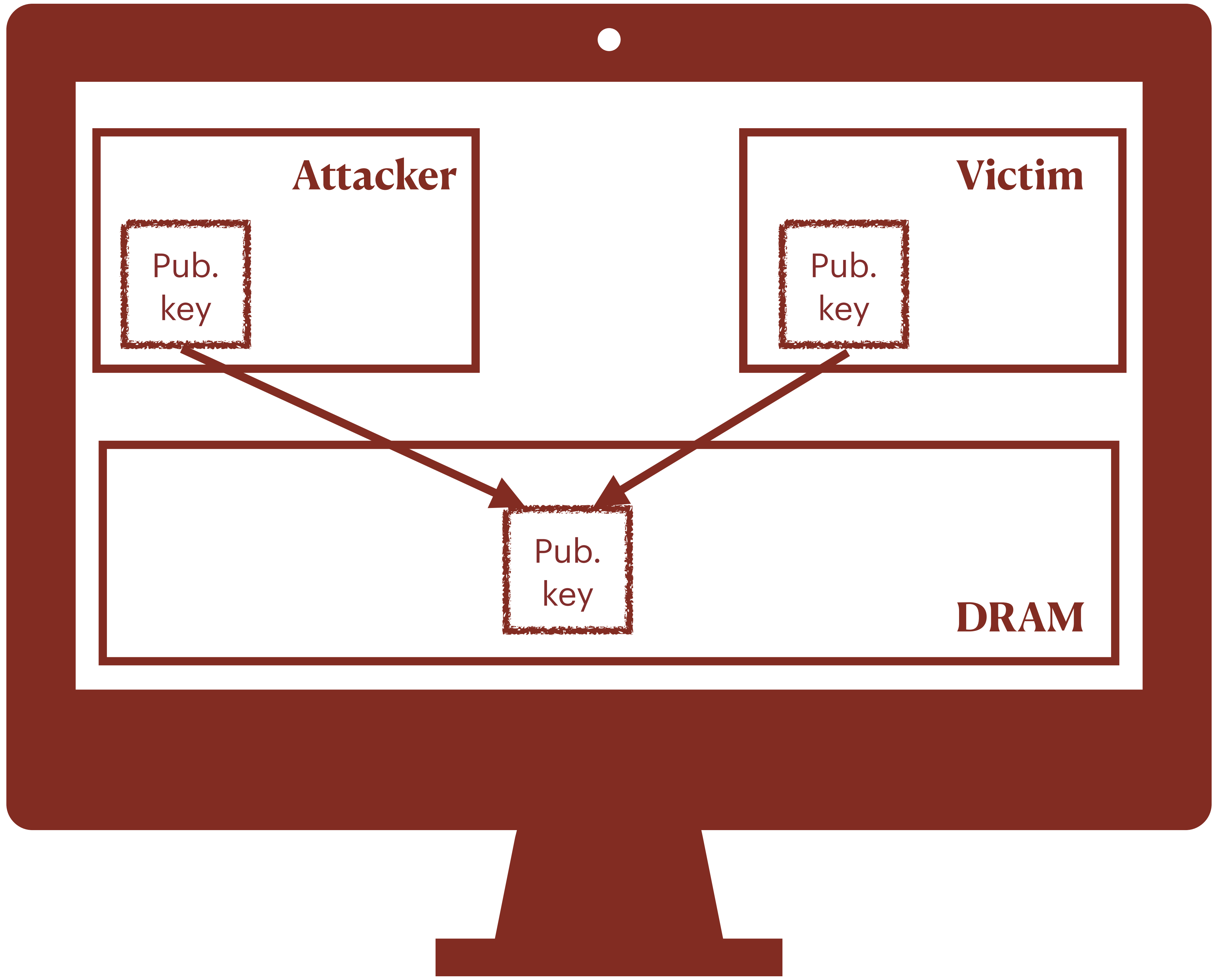


Step 1: Templating

Step 2: Wait for memory deduplication

Step 3: Hammer

Attack variant: Compromising OpenSSH

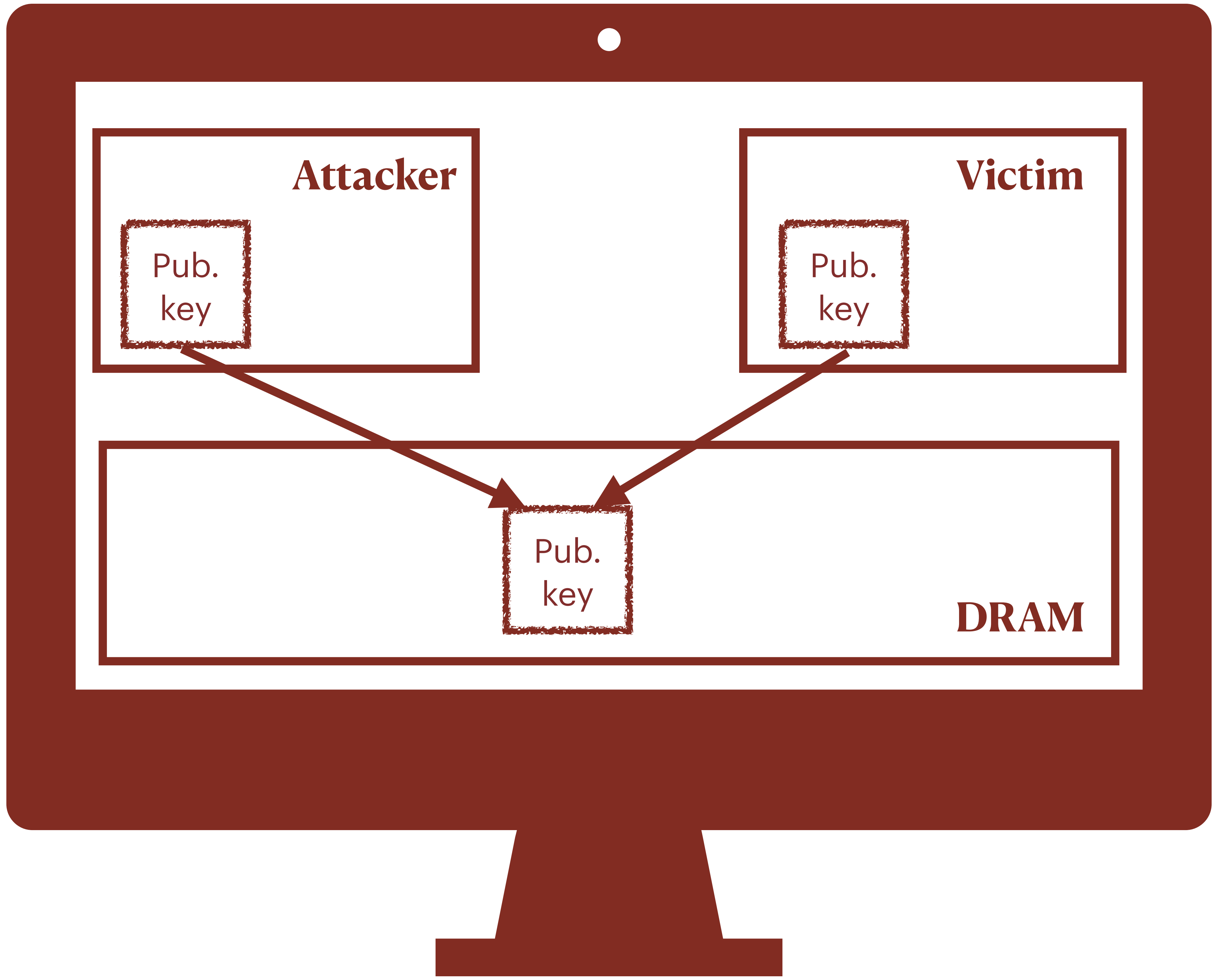


Step 1: Templating

Step 2: Wait for memory deduplication

Step 3: Hammer

Attack variant: Compromising OpenSSH

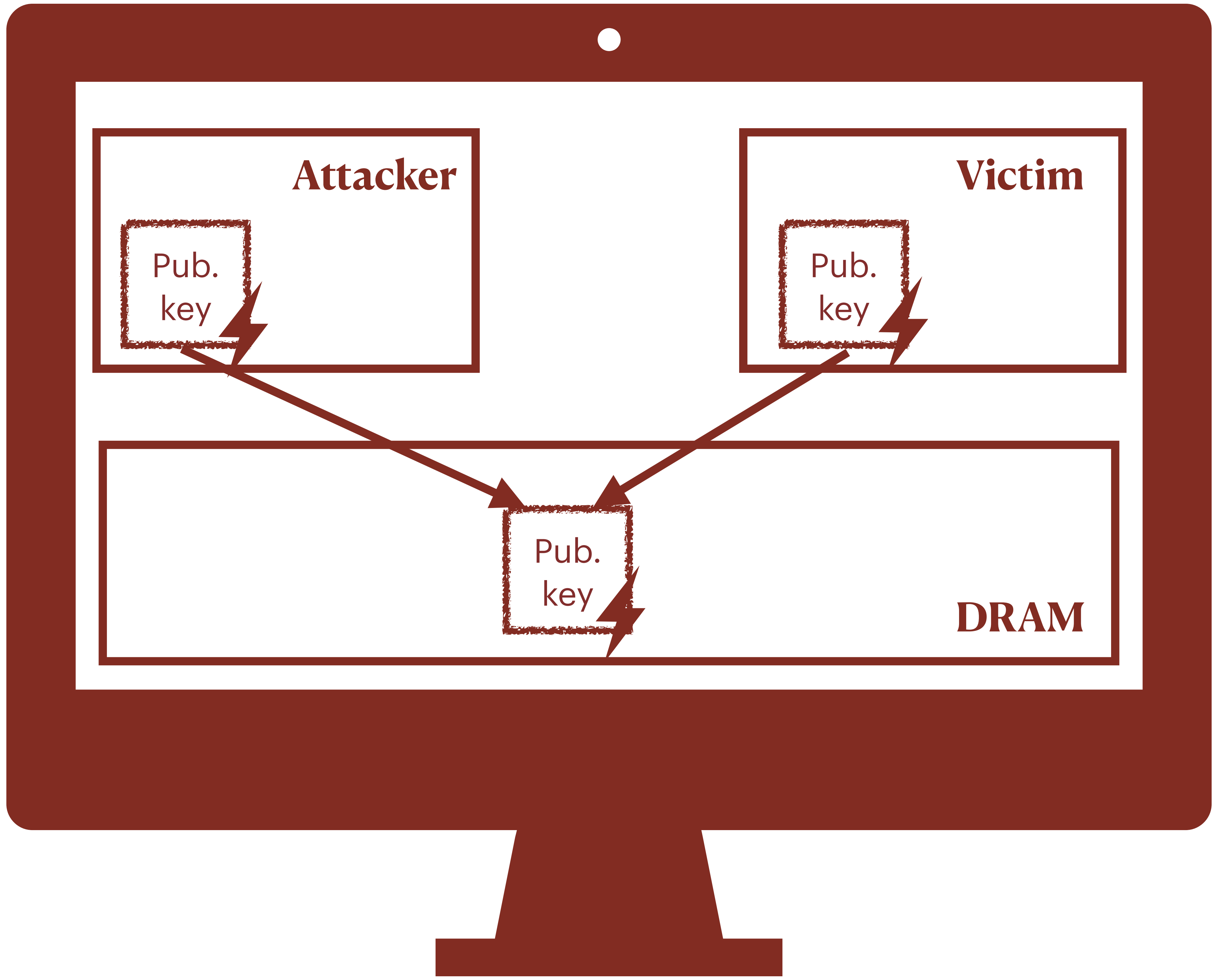


Step 1: Templating

Step 2: Wait for memory deduplication

Step 3: Hammer

Attack variant: Compromising OpenSSH

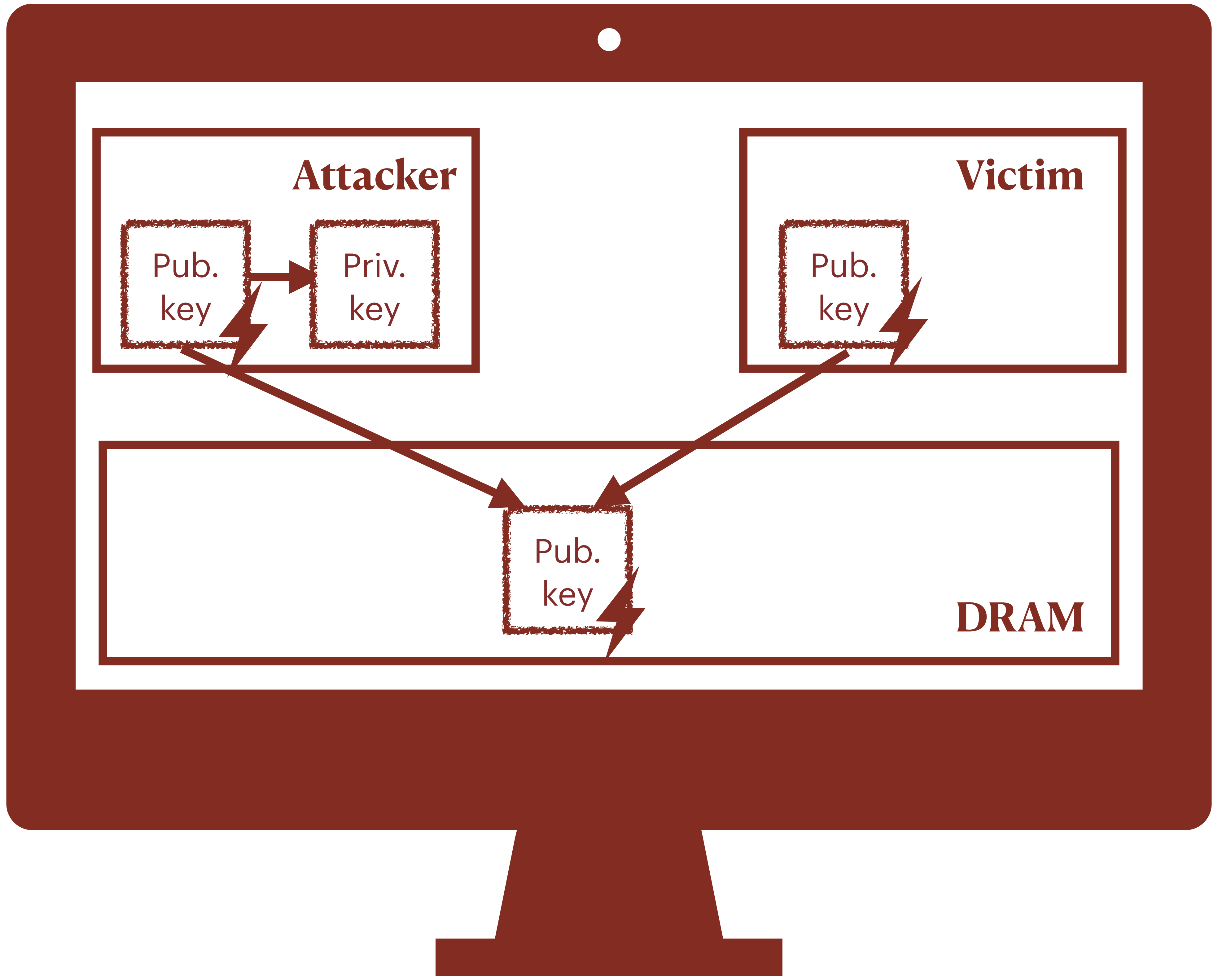


Step 1: Templating

Step 2: Wait for memory deduplication

Step 3: Hammer

Attack variant: Compromising OpenSSH

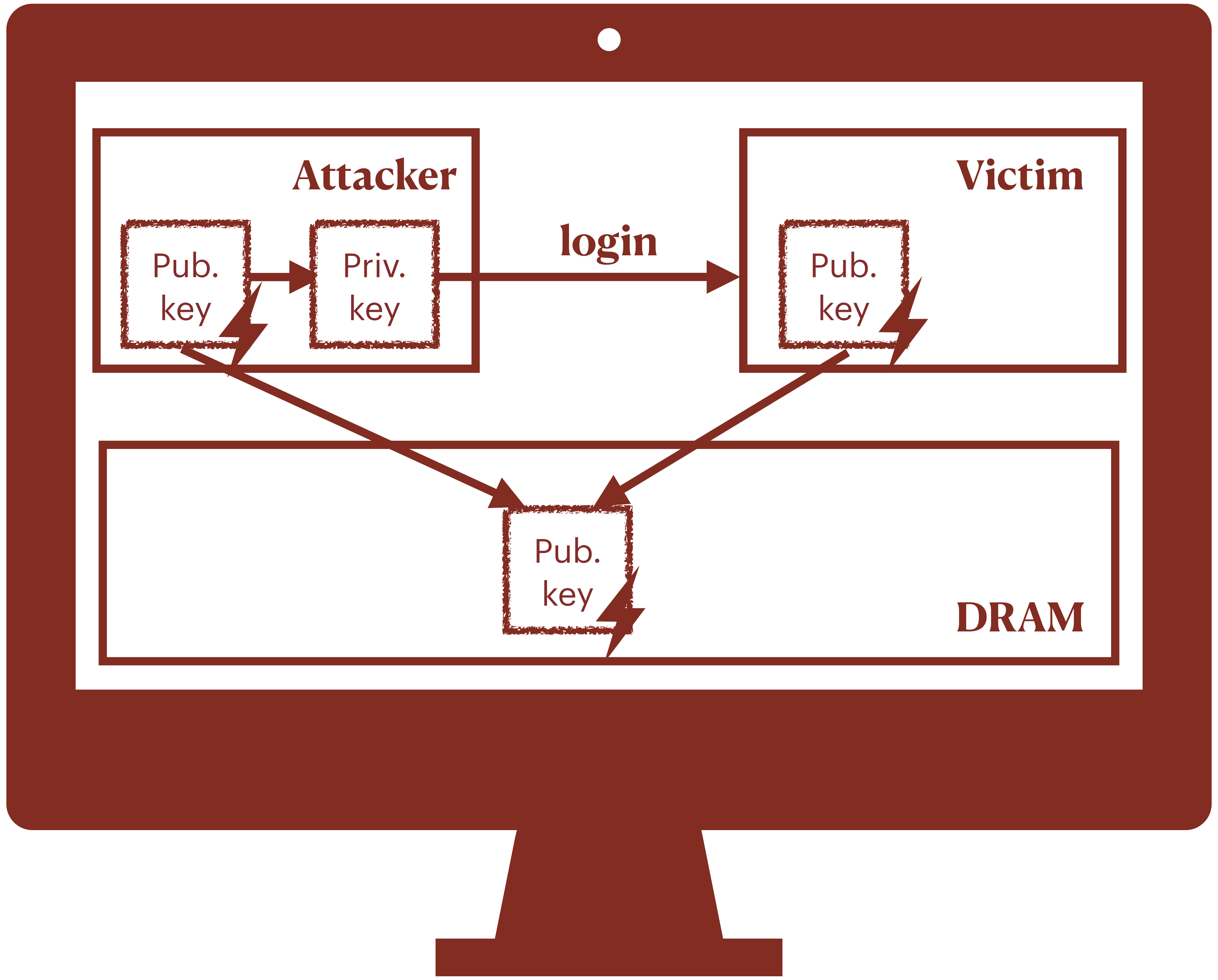


Step 1: Templating

Step 2: Wait for memory deduplication

Step 3: Hammer

Attack variant: Compromising OpenSSH



Step 1: Templating

Step 2: Wait for memory deduplication

Step 3: Hammer

Discussion

- A practical high-impact exploit of the Rowhammer vulnerability
- Deep analysis of RSA under a bit flip
- Still works on DDR4[1], and maybe even DDR5[2]

- Relies heavily on memory deduplication
- Highly dependent on exact implementation of Linux's Kernel Same-page Merging (KSM) and Transparent HugePages (THP)
- Does not discuss other applications than RSA
  - Instructions?
  - PTE?

[1] Frigo, Pietro, et al. "TRRespass: Exploiting the many sides of target row refresh." *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2020.

[2] Jattke, Patrick, et al. "ZenHammer: Rowhammer Attacks on AMD Zen-based Platforms." *33rd USENIX Security Symposium (USENIX Security 2024)*. 2024.APA

Conclusion

- Flip Feng Shui shows that it is practical to exploit Rowhammer
- Attacker can log into a co-resident victim VM
- Highly dependent on memory deduplication
  - Likely not possible anymore in cloud