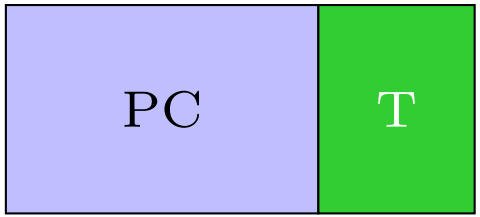


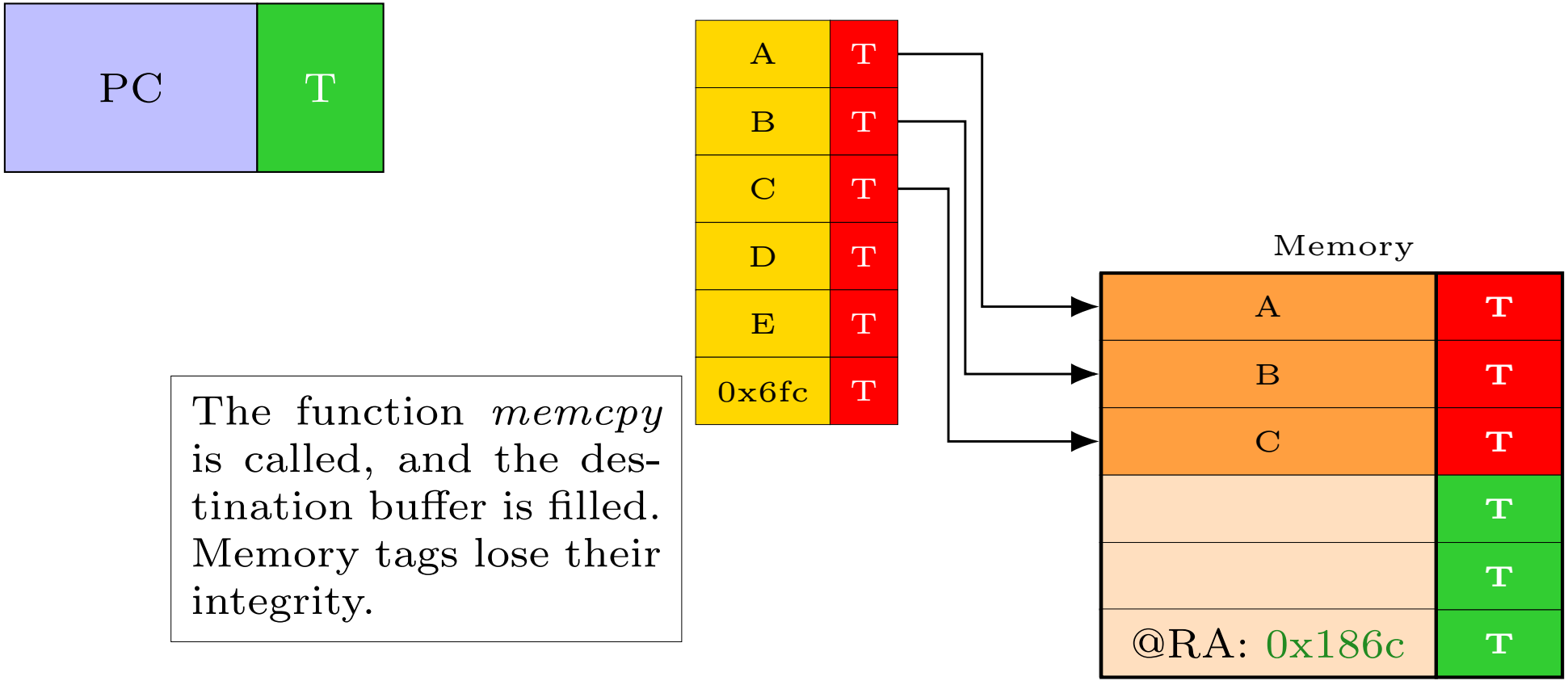
Source buffer

A	T
B	T
C	T
D	T
E	T
0x6fc	T

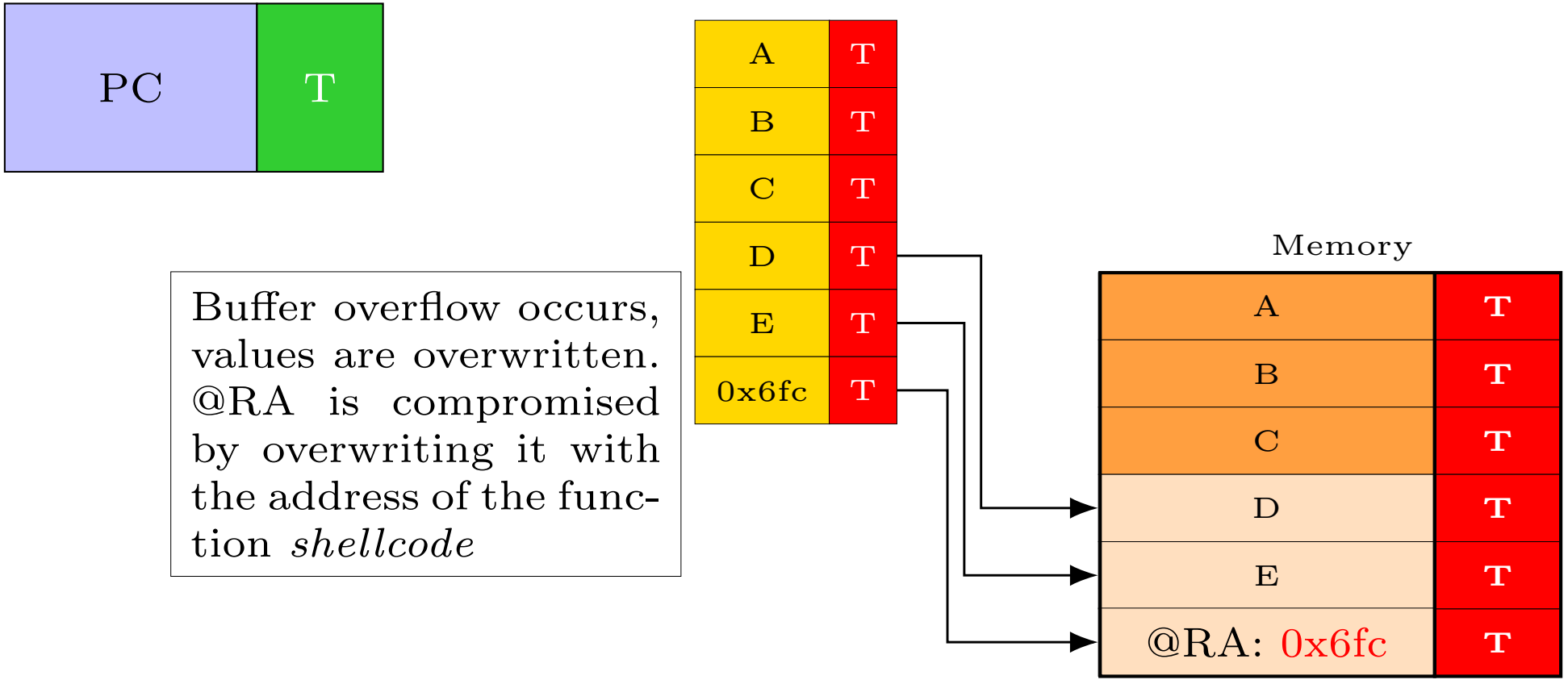
The source buffer is initialised, the destination buffer is empty and the return address (@RA) is trusted.

Memory

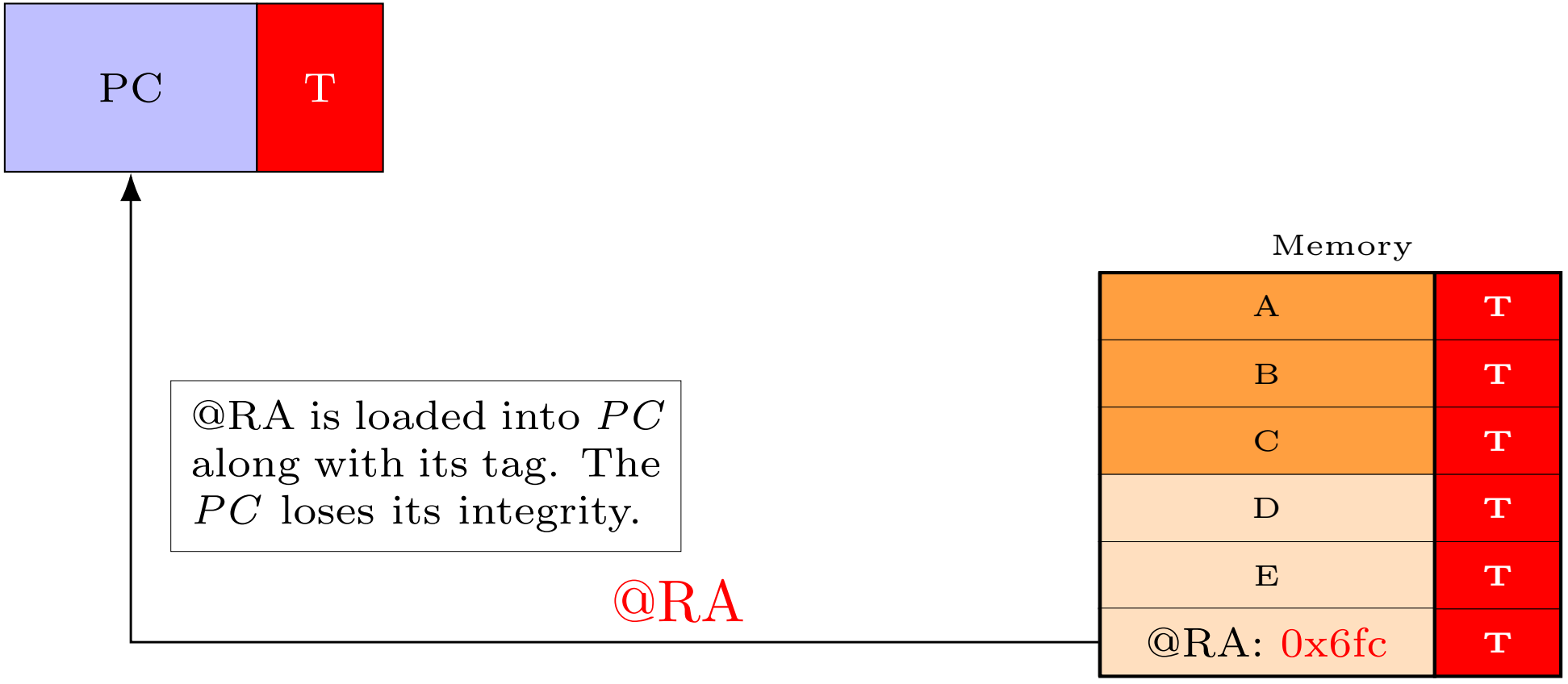
	T
Destination buffer	T
	T
	T
	T
@RA: 0x186c	T

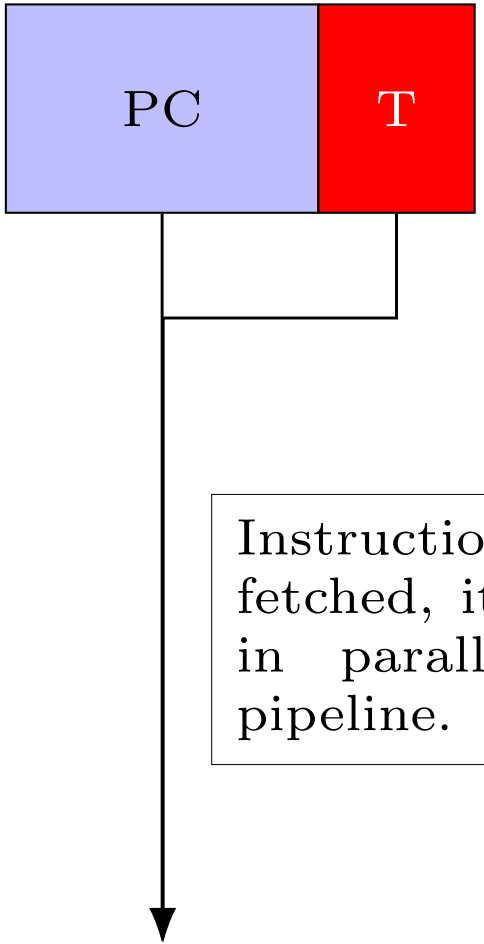


The function *memcpy* is called, and the destination buffer is filled. Memory tags lose their integrity.



Buffer overflow occurs, values are overwritten. @RA is compromised by overwriting it with the address of the function *shellcode*


PC
T
@RA is loaded into PC along with its tag. The PC loses its integrity.
@RA
Memory
A
T
B
T
C
T
D
T
E
T
@RA: 0x6fc
T



Instruction *shellcode* is fetched, its tag is sent in parallel into the pipeline.

Memory

A	T
B	T
C	T
D	T
E	T
@RA: 0x6fc	T