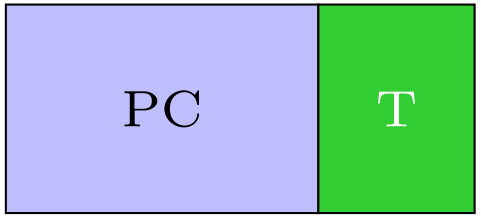
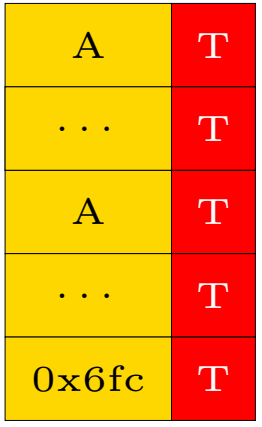
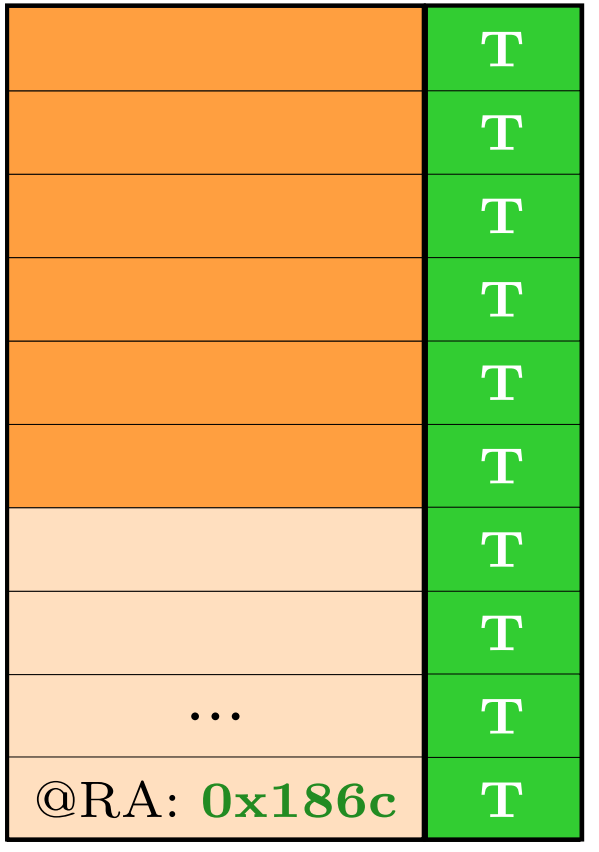
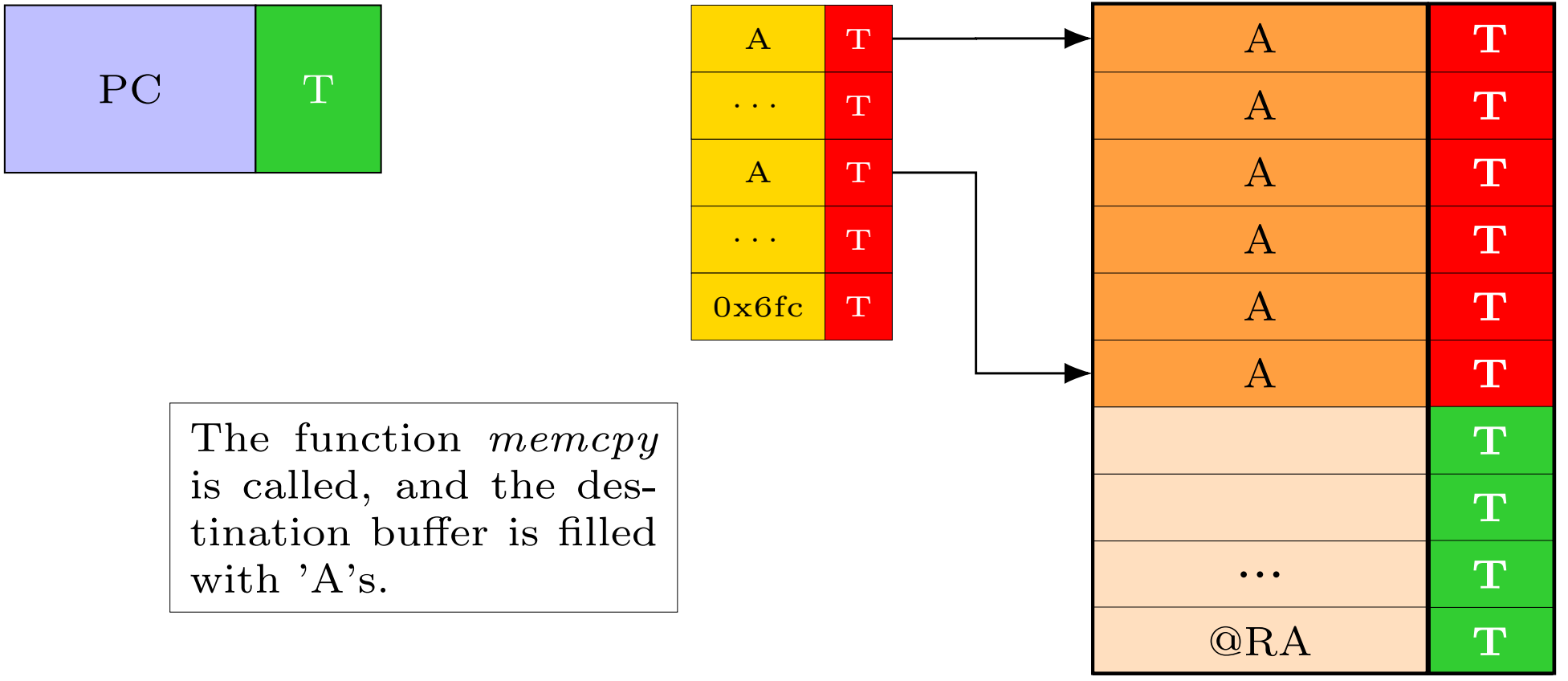


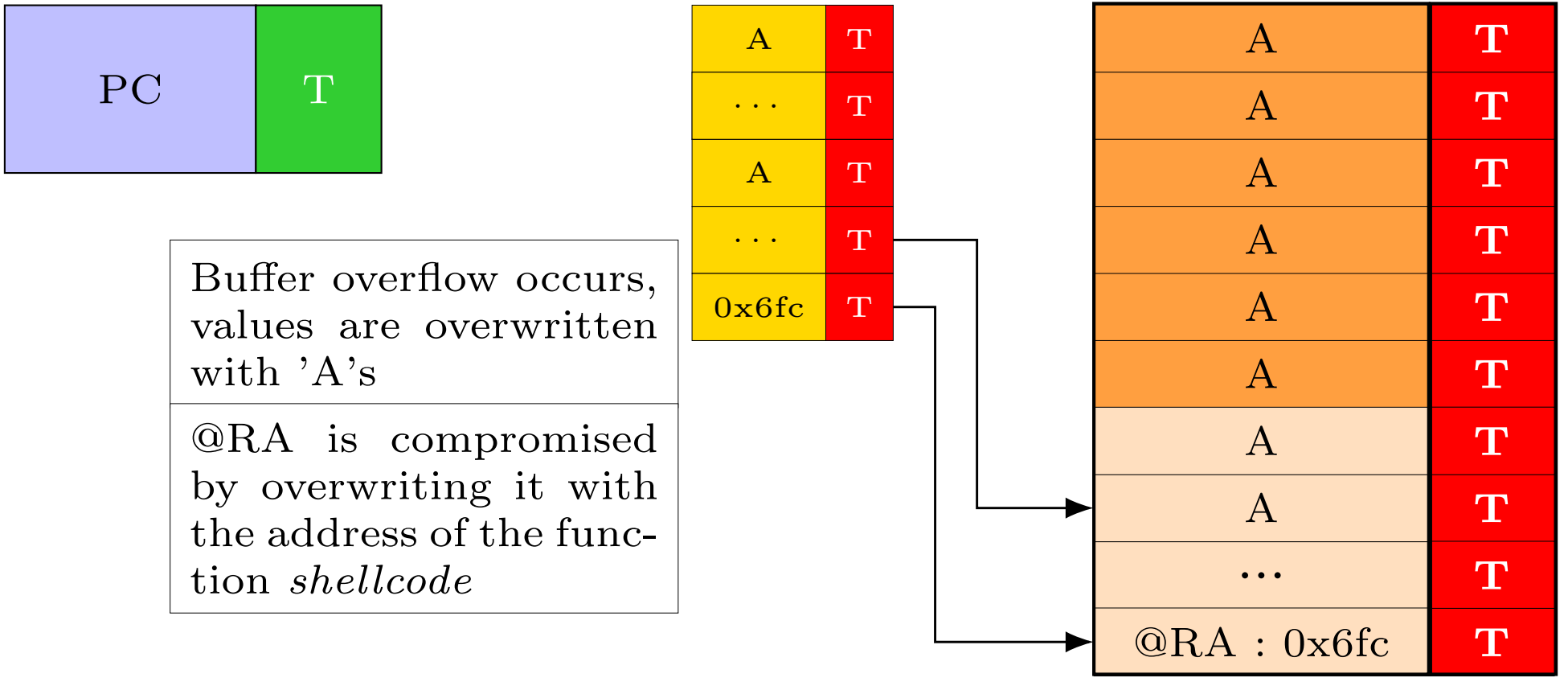


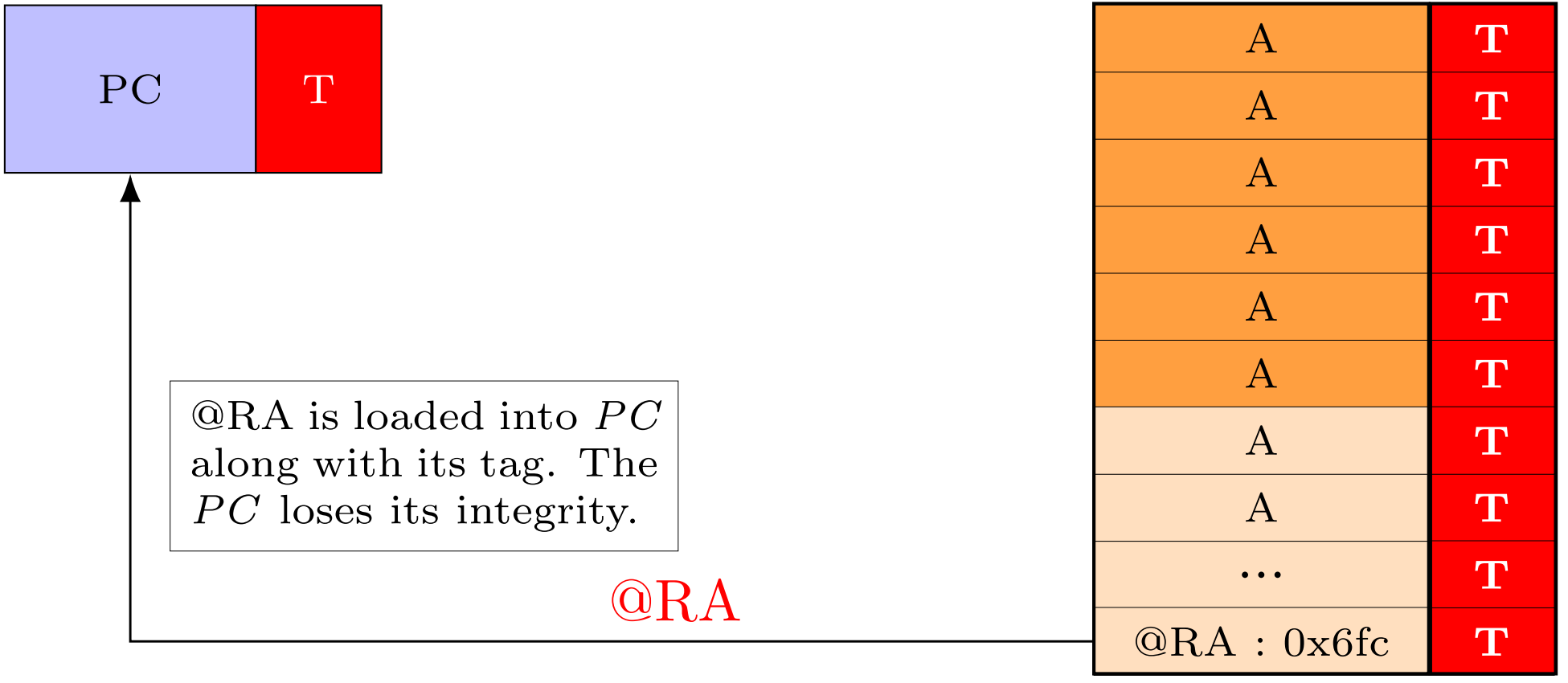
The source buffer is initialised, the destination buffer is empty and the return address (@RA) is trusted.

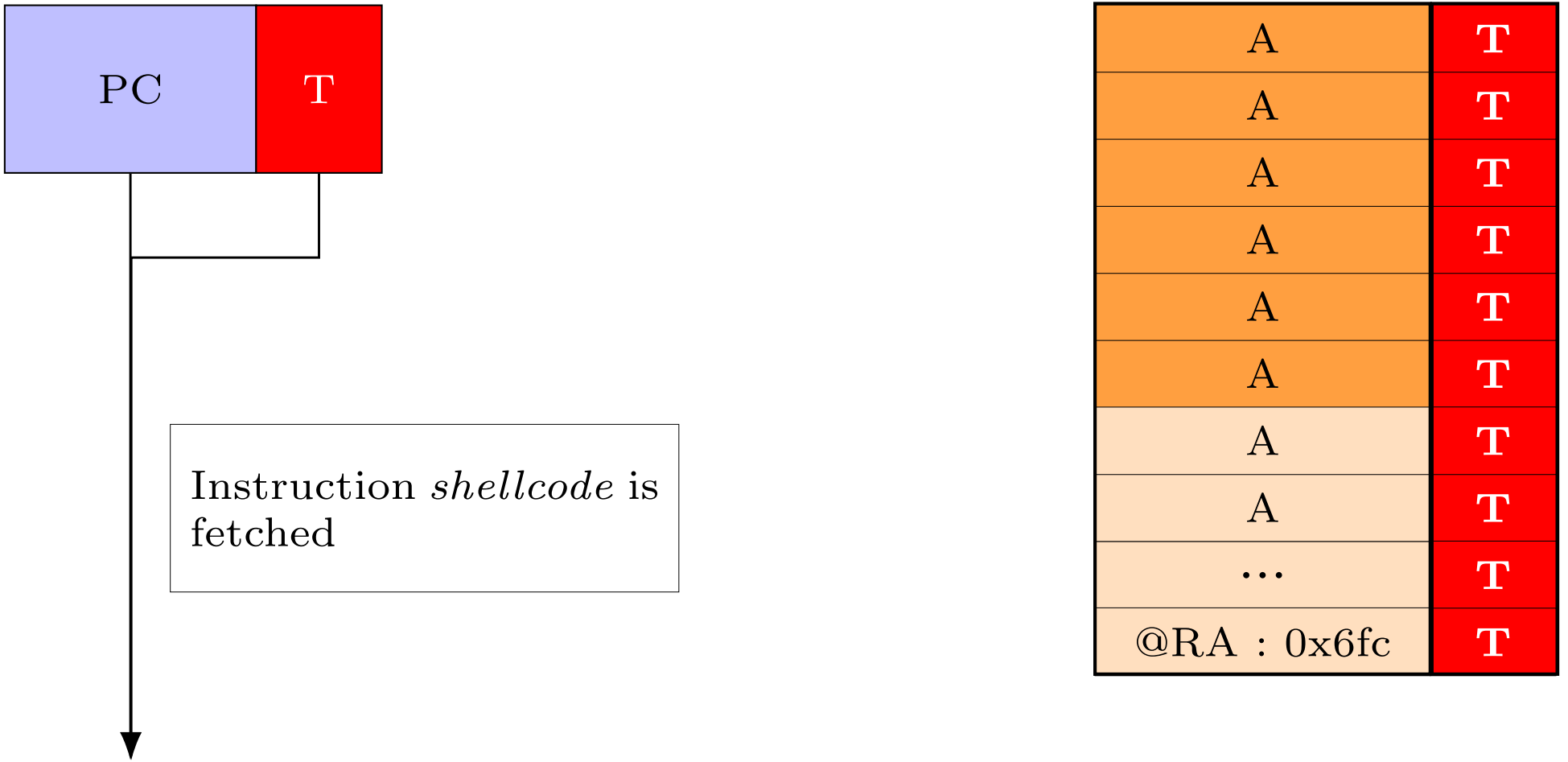




The function *memcpy* is called, and the destination buffer is filled with 'A's.


PC
T
A
T
...
T
A
T
...
T
0x6fc
T
A
T
A
T
A
T
A
T
A
T
A
T
A
T
A
T
...
T
@RA : 0x6fc
T
Buffer overflow occurs, values are overwritten with 'A's
@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
A
T
A
T
A
T
A
T
A
T
A
T
A
T
...
T
@RA : 0x6fc
T


PC
T
Instruction *shellcode* is fetched
A
T
A
T
A
T
A
T
A
T
A
T
A
T
...
T
@RA : 0x6fc
T