



A	T
...	T
A	T
...	T
0x6fc	T

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

	T
	T
	T
	T
	T
	T
	T
	T
	T
	T
...	T
@RA: 0x186c	T



A	T
...	T
A	T
...	T
0x6fc	T

Diagram showing a memory stack. The first six rows are orange with red 'T' flags. The next three rows are light orange with green 'T' flags. The last row is light orange with a green 'T' flag. Arrows point from the first and third rows of the source table to the first and sixth rows of this stack.

A	T
A	T
A	T
A	T
A	T
A	T
	T
	T
...	T
@RA	T

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



Buffer overflow occurs,
values are overwritten
with 'A's

@RA is compromised
by overwriting it with
the address of the func-
tion *shellcode*

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



@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
A	T
...	T
@RA : 0x6fc	T



Instruction *shellcode* is
fetched

A	T
A	T
A	T
A	T
A	T
A	T
A	T
A	T
...	T
@RA : 0x6fc	T