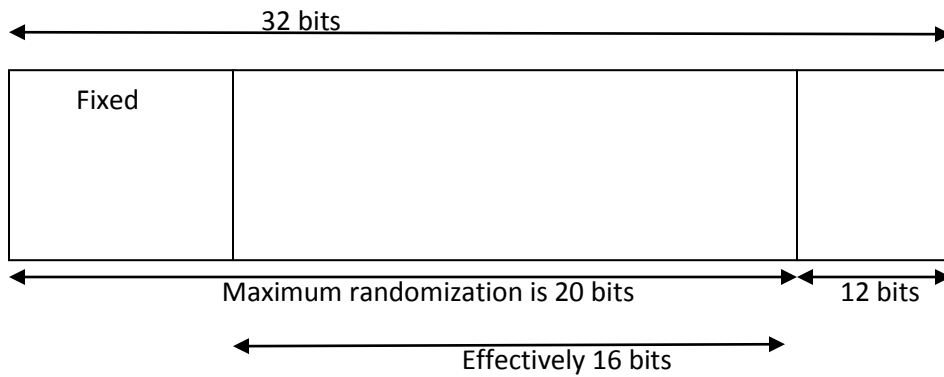
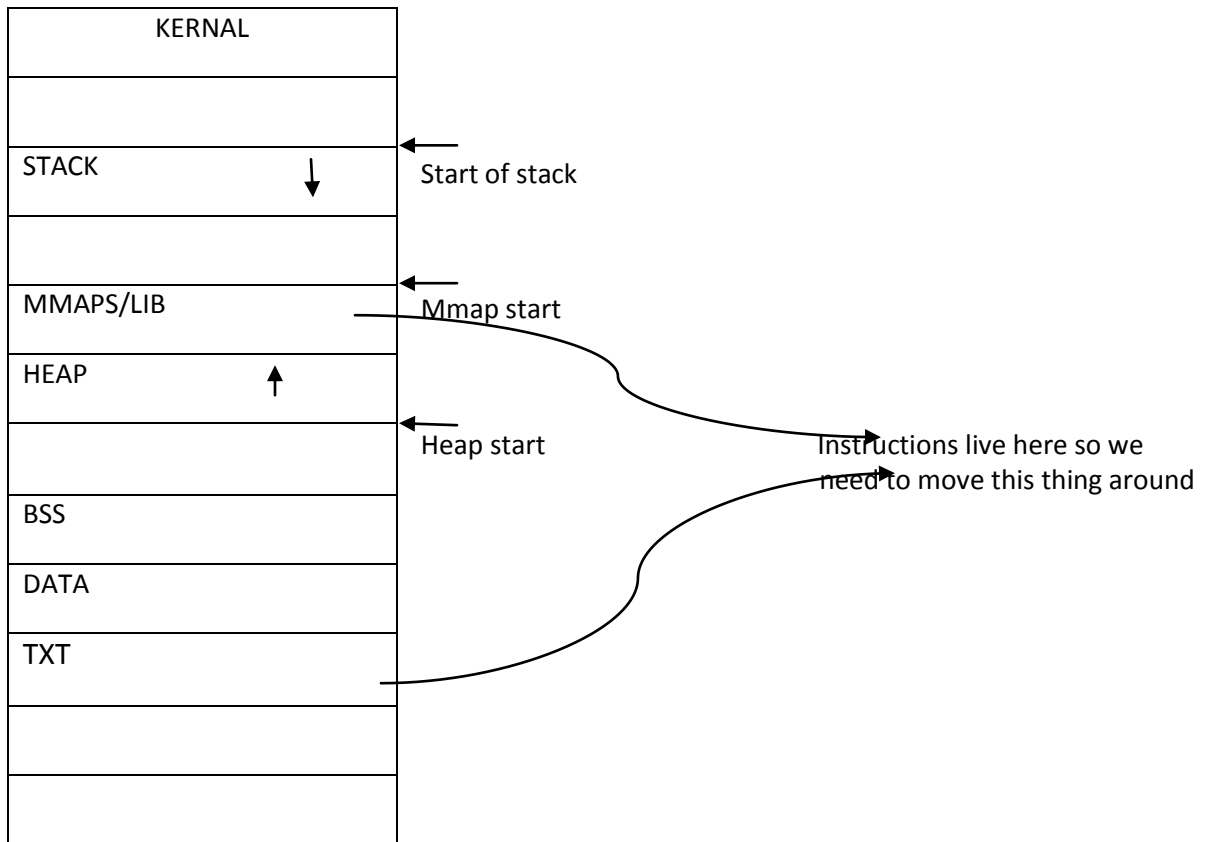


Address Space Randomization:

Assumptions of Buffer Overflow: Attacker knows approximate layout of the memory.

Idea: Take away this knowledge from the attacker



Assumption: Exact Operating system is available with the attacker.
16 bits of randomness is approximately = 4 minutes.
Attacker may not need to guess all randomness.

Fix:

64 bit addressing (Easy fix).

40 bits $\rightarrow 2^{40} \rightarrow$ huge number

All the different randomizations that we can perform:

Internal randomization:

Stack:

- Local variable ordering
- Inter frame padding
- Frame ordering
- Parameter ordering

Code segments:

- Function ordering
- Instruction choices
- Padding
- Basic blocks
- Polymorphic code
- Instruction set randomization

Heap:

- Inter allocation padding
- ordering

From the paper we infer that rearranging does not really help.

If the local user is using the system then compile time randomization will not help

In address space randomization programmer does not need to do anything.