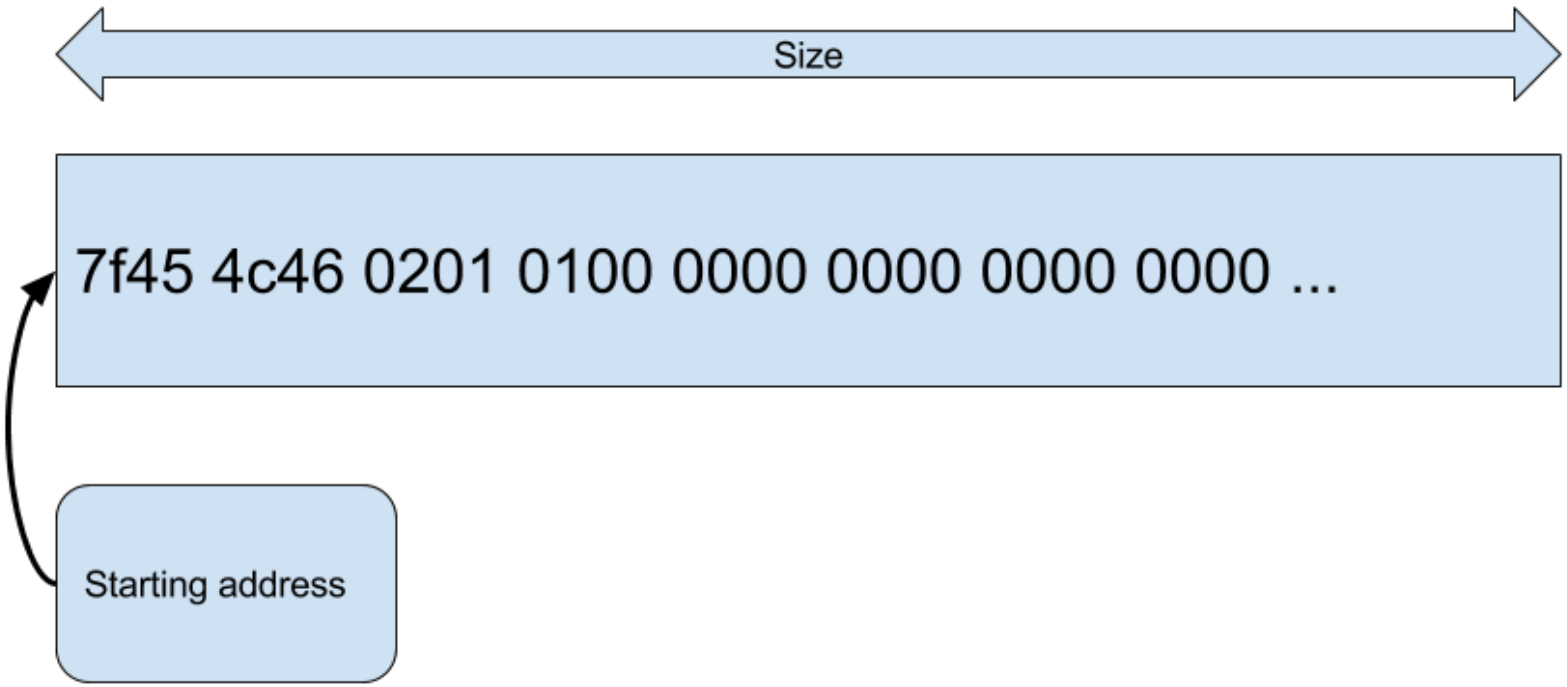
Session 0x06

Buffer Management

Security Summer School

ACS/Ixia/Hexcellents

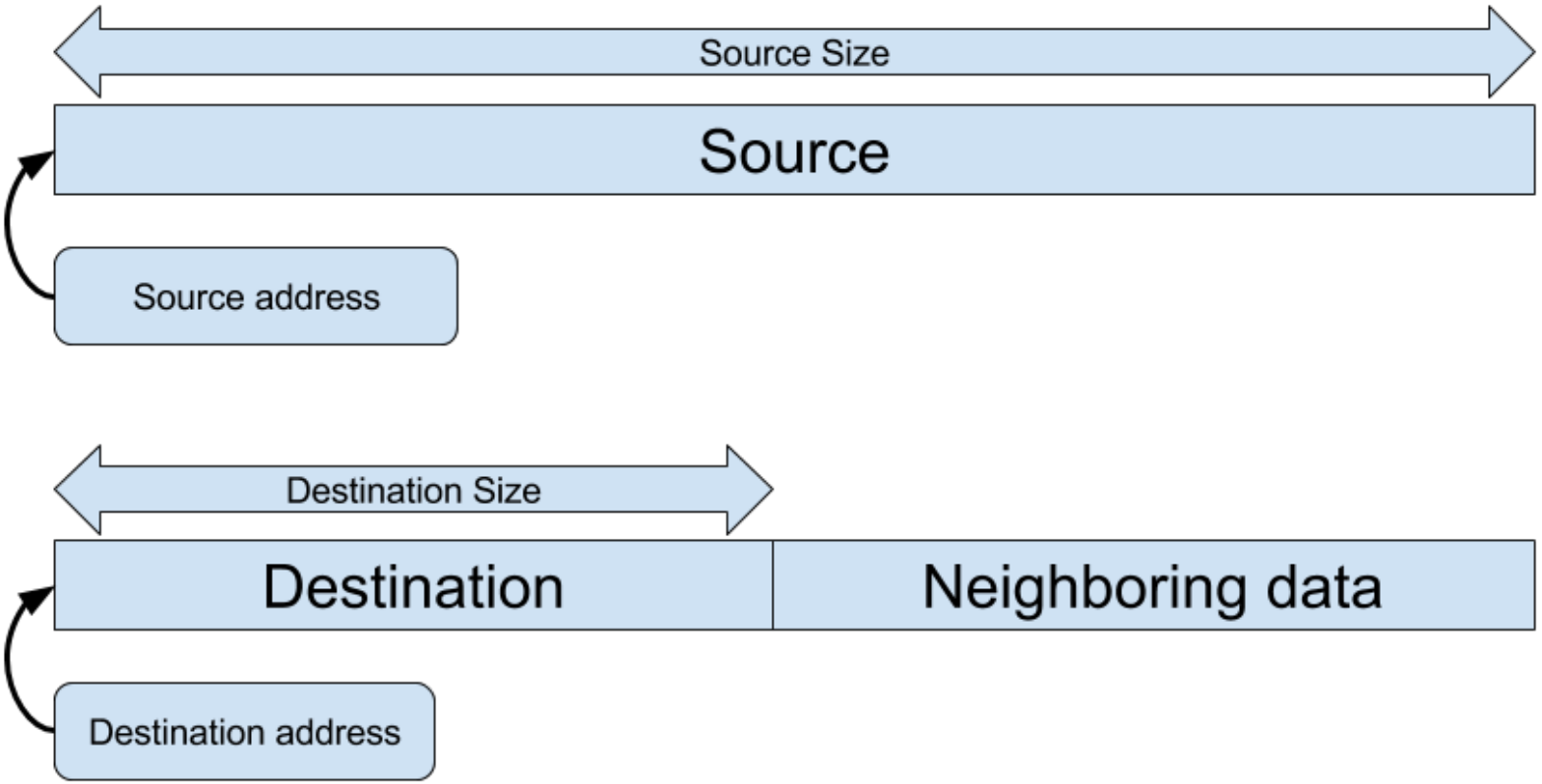
Buffers


Size
7f45 4c46 0201 0100 0000 0000 0000 0000 ...
Starting address

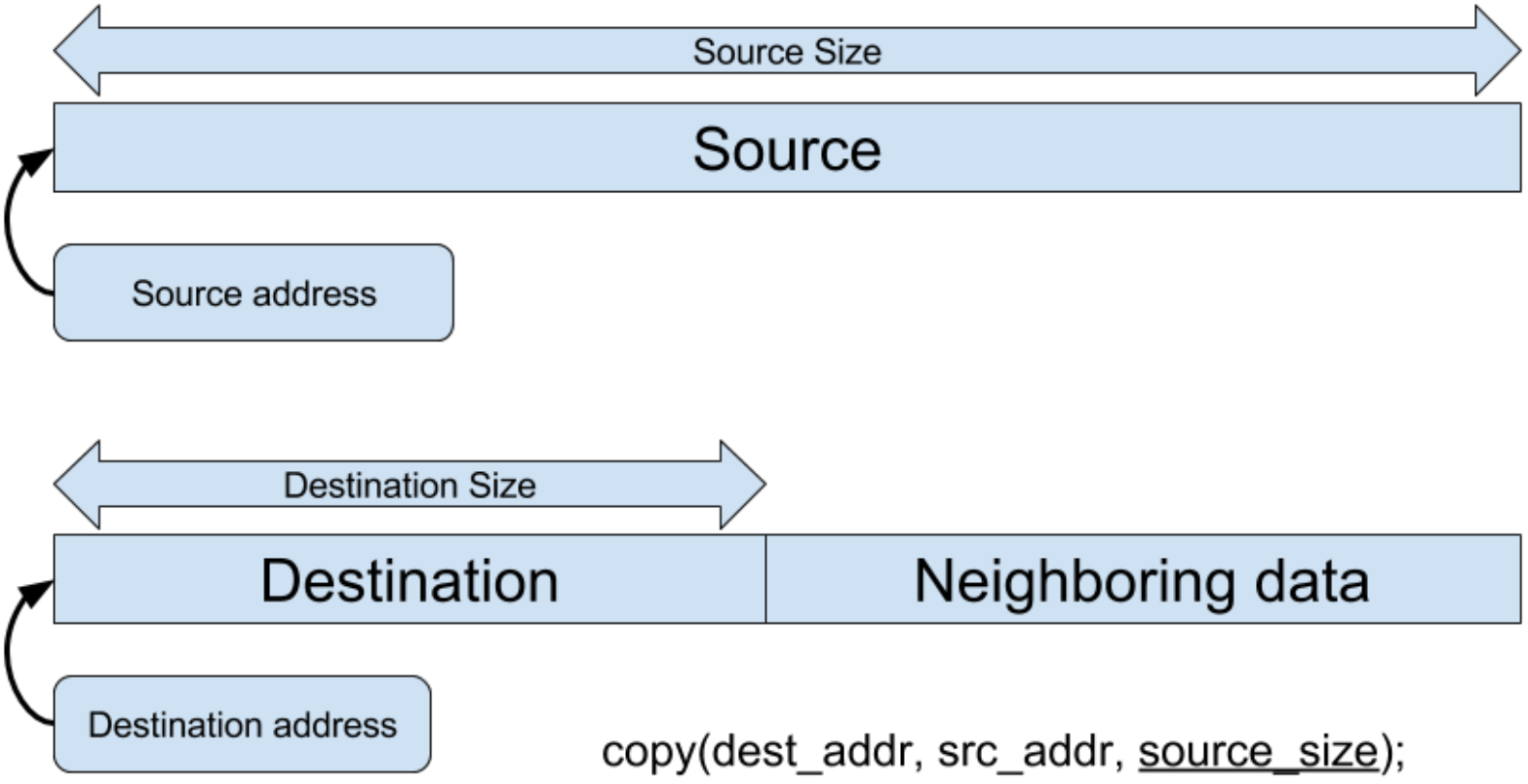
Possible locations

- Stack
- Heap
- .data
- .rodata
- .bss
- ...or any other memory region

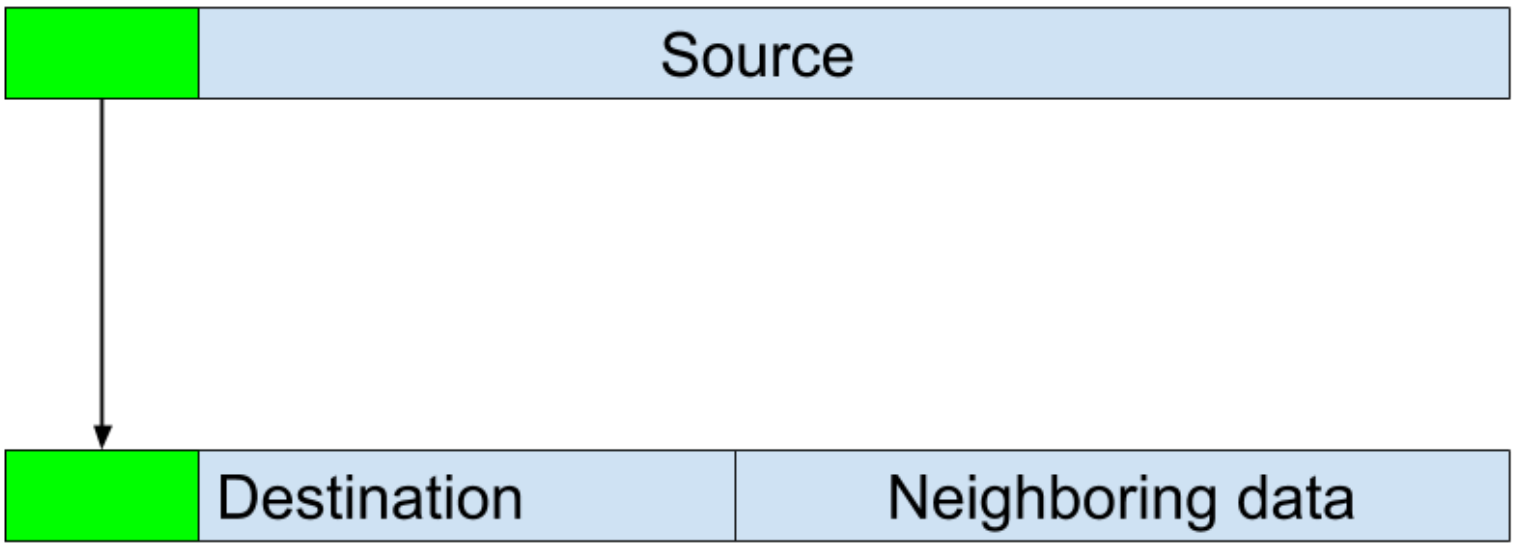
Buffer overflow



Buffer overflow

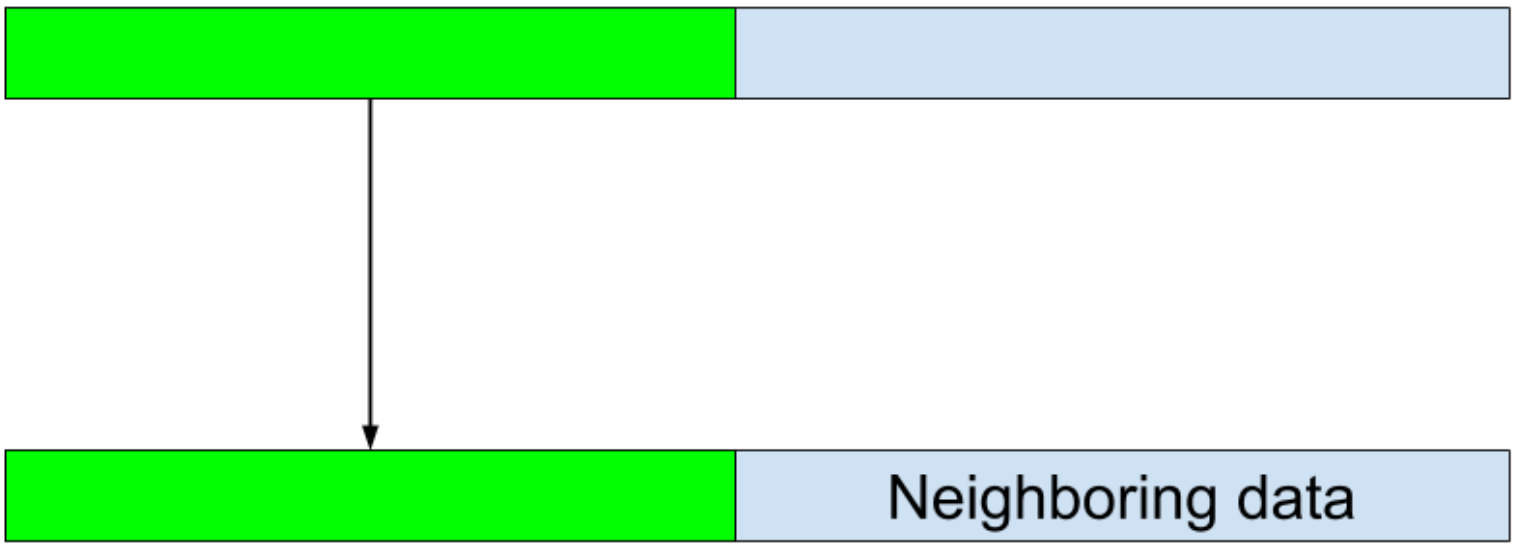


Buffer overflow



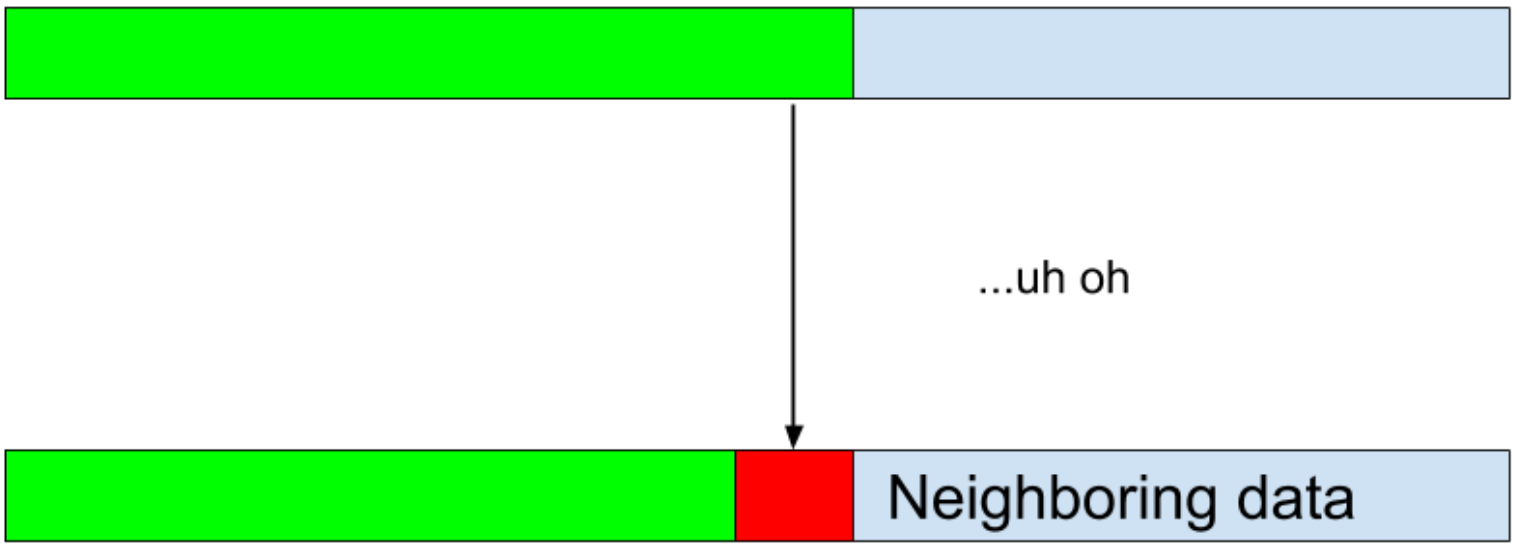
copy(dest_addr, src_addr, source_size);

Buffer overflow



copy(dest_addr, src_addr, source_size);

Buffer overflow



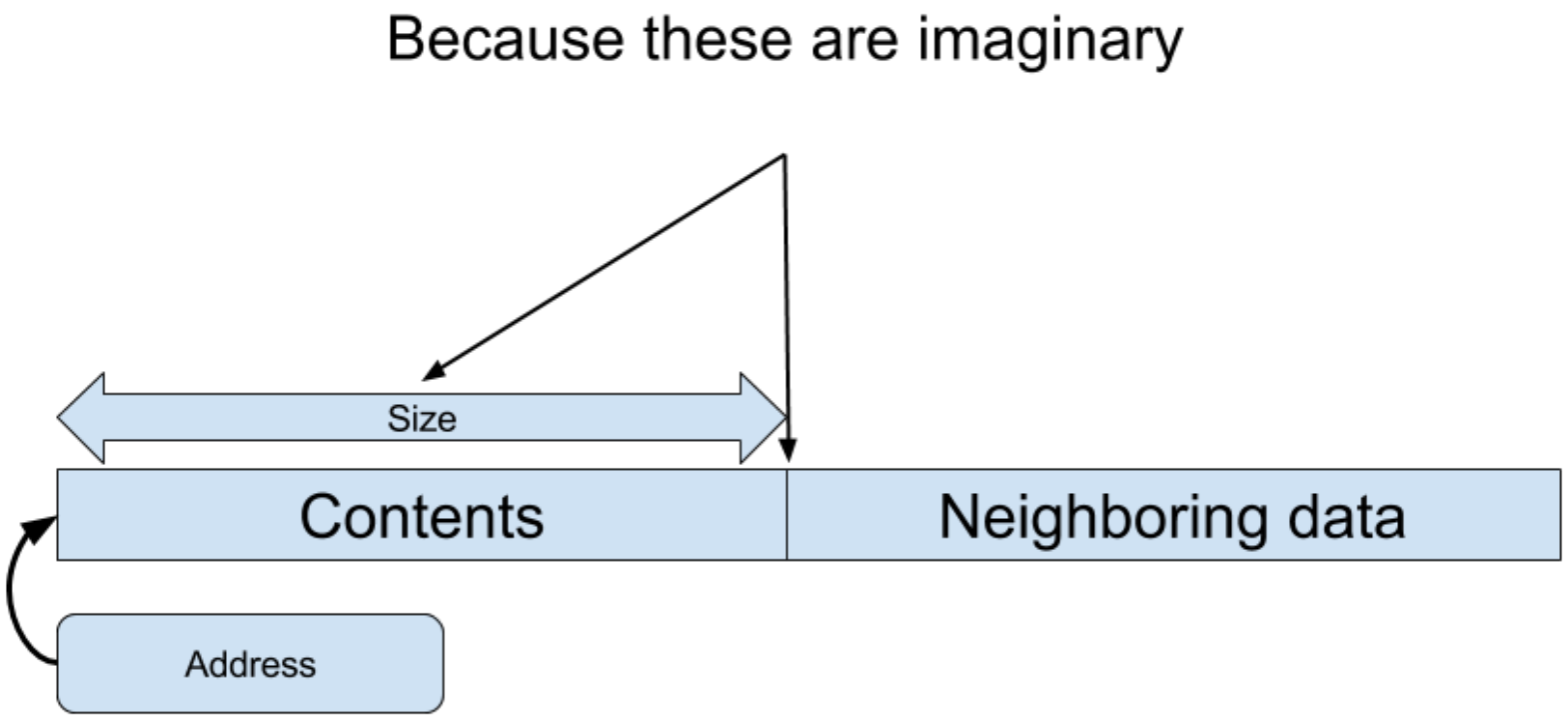
copy(dest_addr, src_addr, source_size);

Buffer overflow

- Why is this possible?

Buffer overflow

- Why is this possible?



Buffer overflow

- Can anyone tell me where my buffers start and end?
- ...and their size?

```
00 00 00 00 00 00 00 00-48 65 6c 6c 6f 20 57 6f  ........Hello Wo
72 6c 64 21 00 00 00 00-54 68 69 73 20 69 73 20  rld!....This is
74 68 65 20 73 65 63 6f-6e 64 20 62 75 66 66 65  the second buffe
72 00 00 00                                      r...
```

Buffer overflow

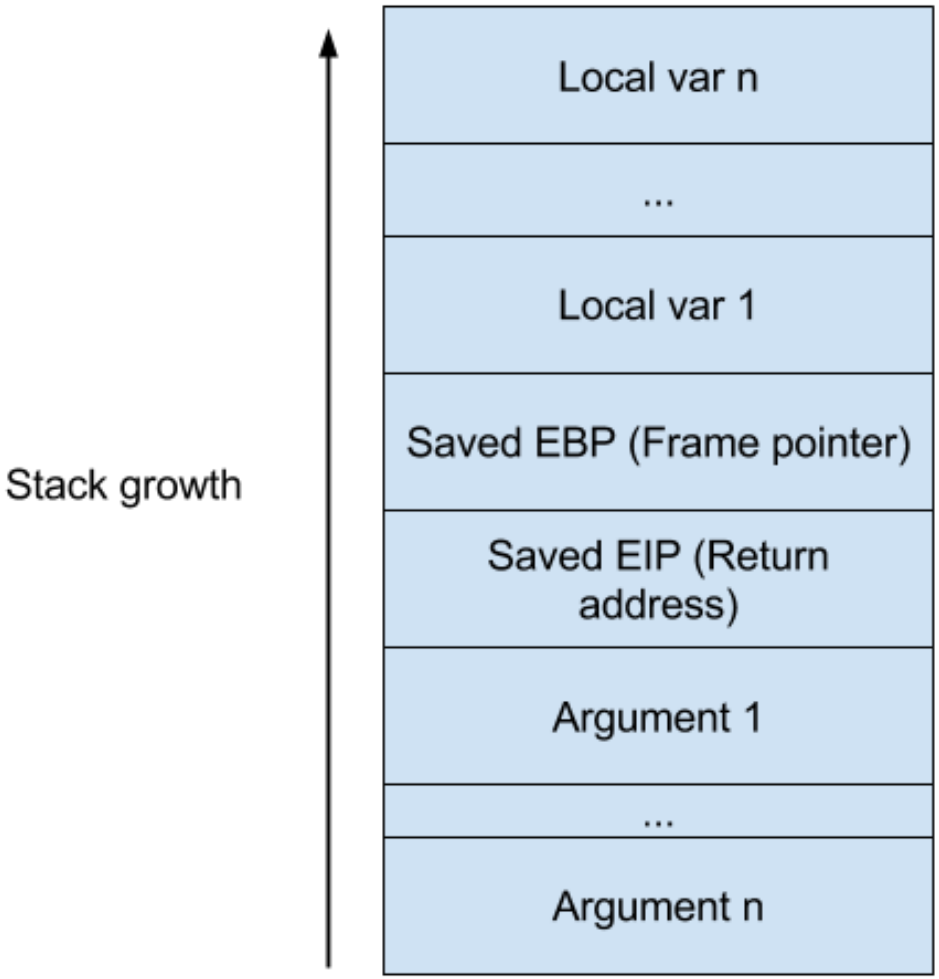
- Can anyone tell me where my buffers start and end?
- ...and their size?

```
00 00 00 00 00 00 00 00-48 65 6c 6c 6f 20 57 6f  ........Hello Wo
72 6c 64 21 00 00 00 00-54 68 69 73 20 69 73 20  rld!....This is
74 68 65 20 73 65 63 6f-6e 64 20 62 75 66 66 65  the second buffe
72 00 00 00                                      r...
```

- Did you guess correctly?

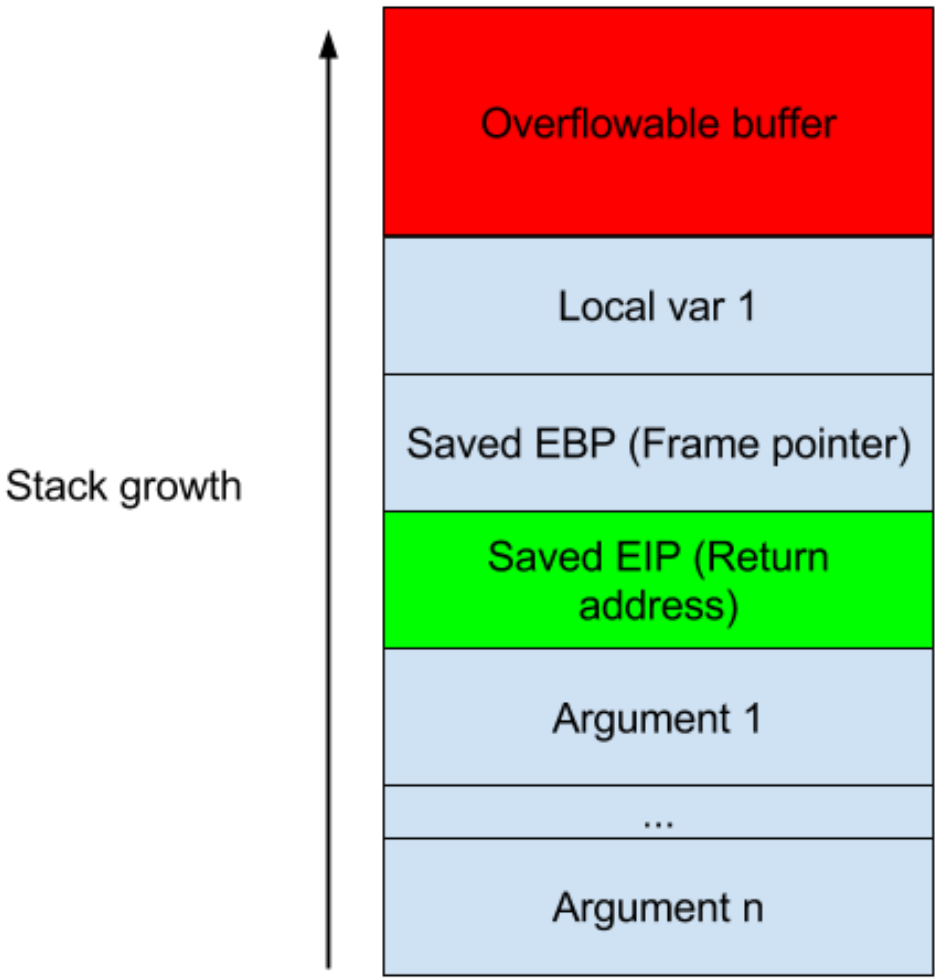
```
char buffer1[6] = "Hello ";
char buffer2[2] = "Wo";
char buffer3[5] = "rld!\0";
char buffer4[12] = "This is the ";
char buffer5[14] = "second buffer\0";
```

The stack - brief reminder

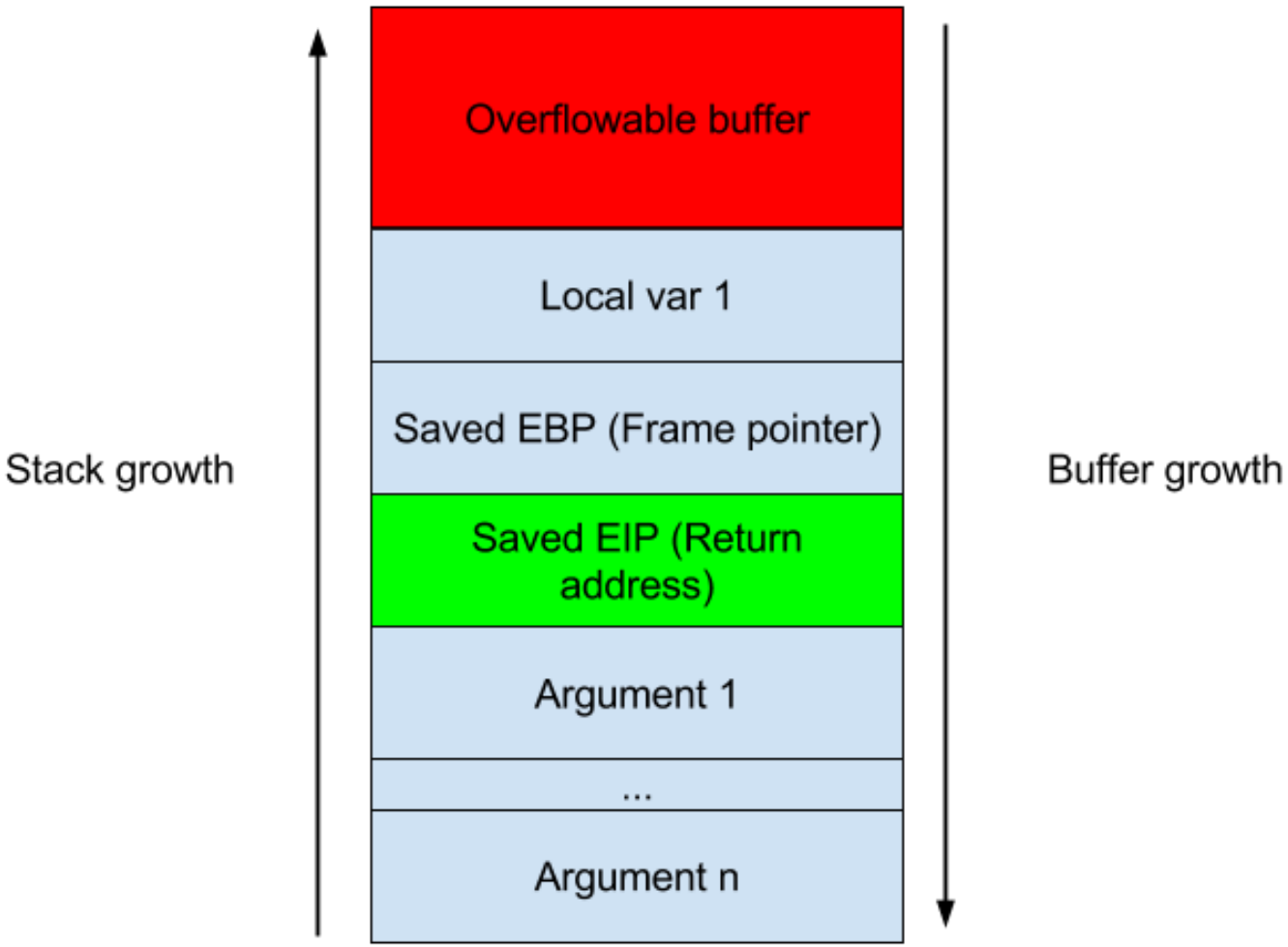


Stack buffer overflows

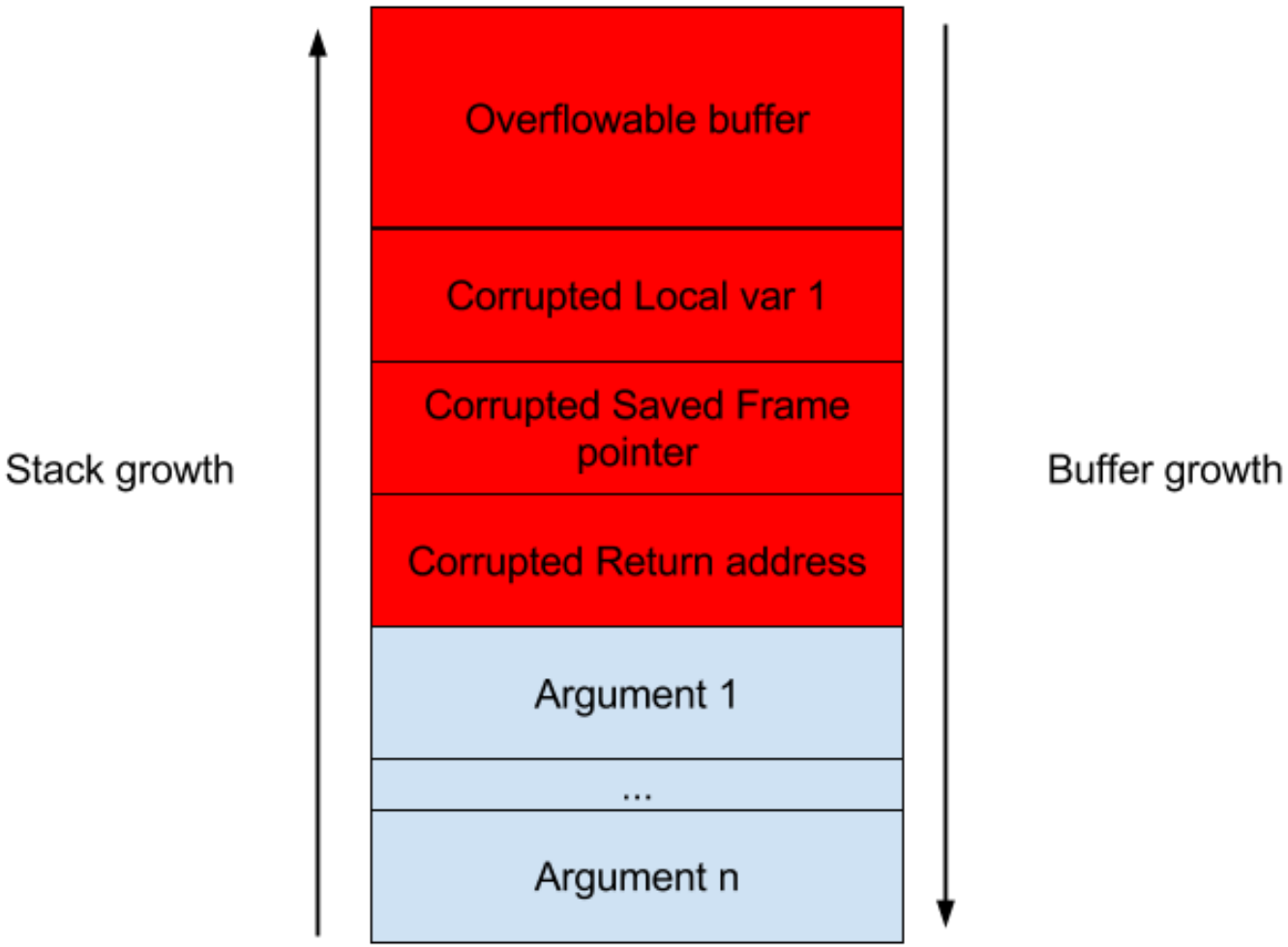
- What if?



Stack buffer overflows



Stack buffer overflows



What causes overflows?

- Hackers?

What causes overflows?

- Hackers?
  - Well, they do trigger them, but they aren't the ones allowing them to happen.

What causes overflows?

- Hackers?
  - Well, they do trigger them, but they aren't the ones allowing them to happen.
- Bad programming languages?

What causes overflows?

- Hackers?
  - Well, they do trigger them, but they aren't the ones allowing them to happen.
- Bad programming languages?
  - Programming languages aren't "bad". Computers do precisely what they are told.
  - Java/Rust/Python isn't the solution to every problem.

What causes overflows?

- Hackers?
  - Well, they do trigger them, but they aren't the ones allowing them to happen.
- Bad programming languages?
  - Programming languages aren't "bad". Computers do precisely what they are told.
  - Java/Rust/Python isn't the solution to every problem.
- Bad programmers?

What causes overflows?

- Hackers?
  - Well, they do trigger them, but they aren't the ones allowing them to happen.
- Bad programming languages?
  - Programming languages aren't "bad". Computers do precisely what they are told.
  - Java/Rust/Python isn't the solution to every problem.
- Bad programmers?
  - It's mostly true that coding during Christmas at 1 a.m. is a very bad idea.

What causes overflows?

- Hackers?
  - Well, they do trigger them, but they aren't the ones allowing them to happen.
- Bad programming languages?
  - Programming languages aren't "bad". Computers do precisely what they are told.
  - Java/Rust/Python isn't the solution to every problem.
- Bad programmers?
  - It's mostly true that coding during Christmas at 1 a.m. is a very bad idea.
- No bounds checking?