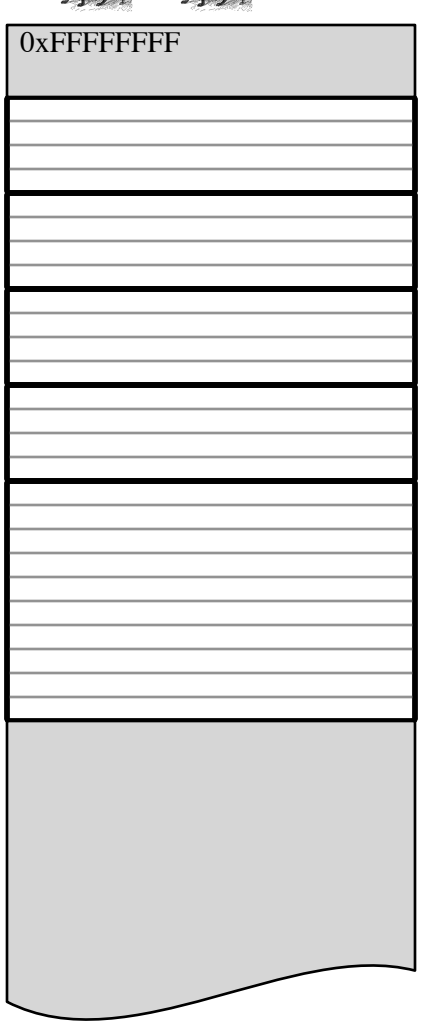
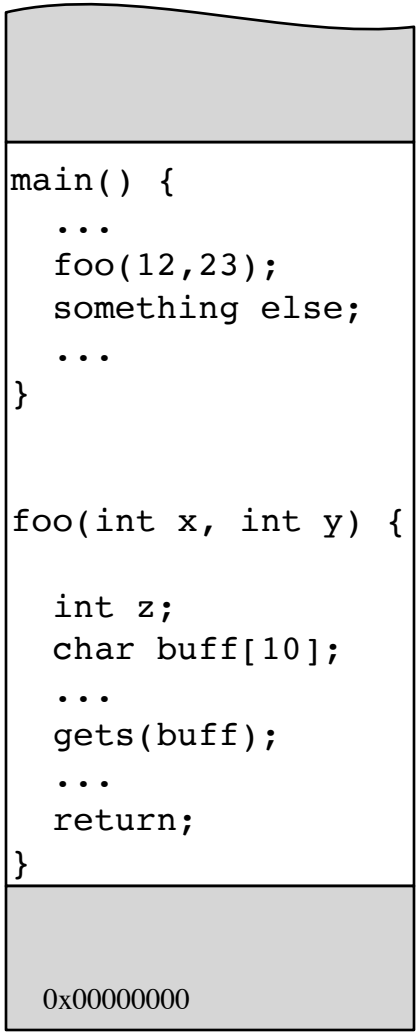
Buffer Overflow!

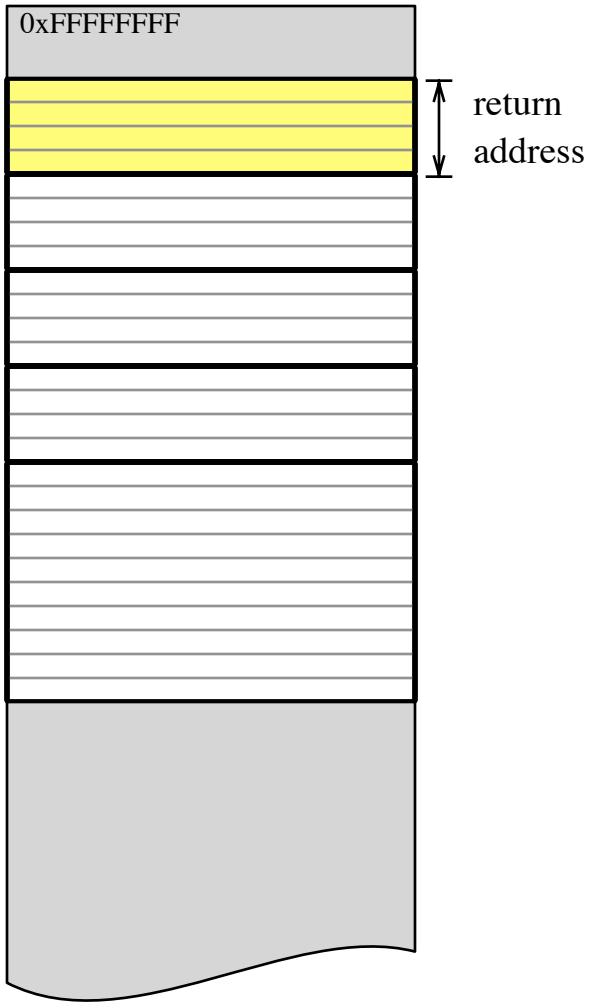
- Thanks to Sean Smith (Dartmouth)

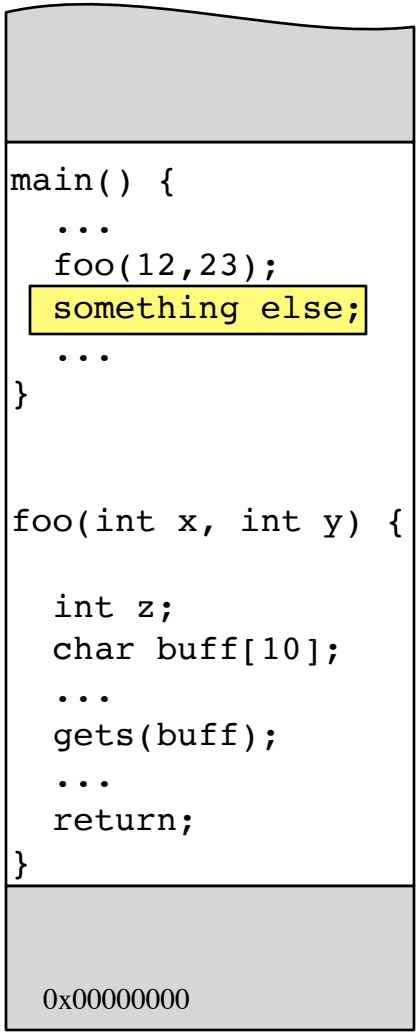
Buffer Overflow



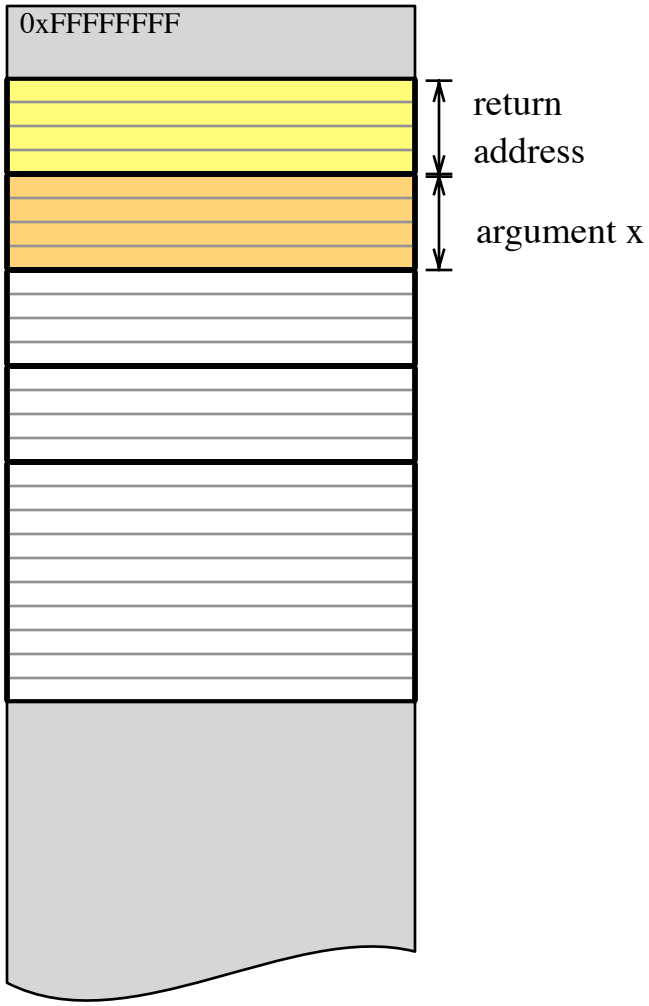


Buffer Overflow





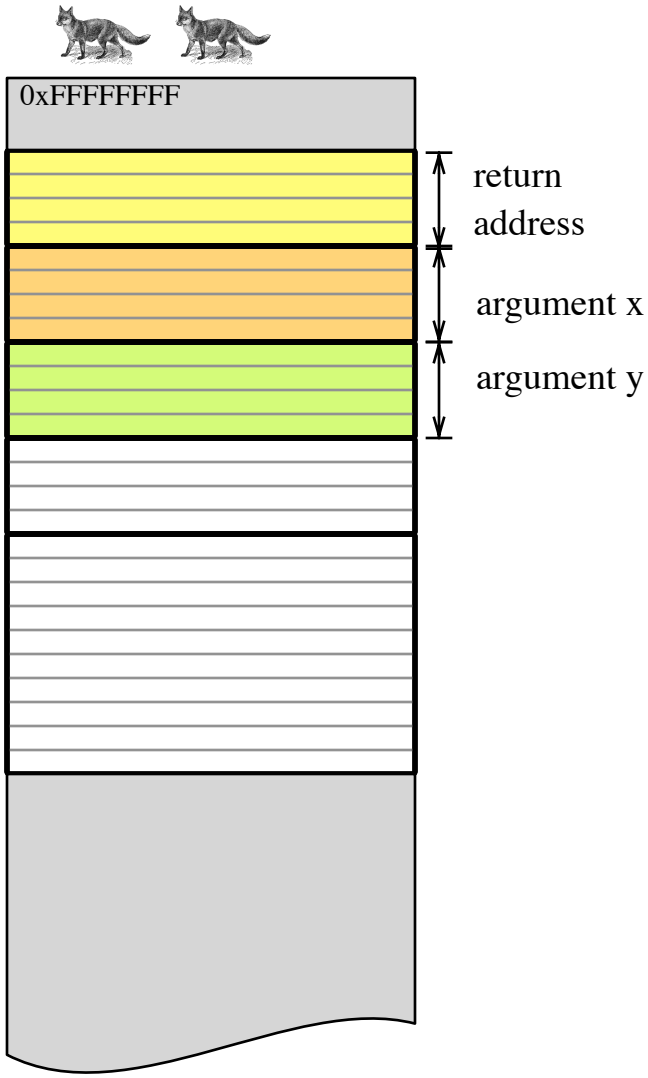
Buffer Overflow



```
main() {
  ...
  foo(12,23);
  something else;
  ...
}


foo(int x, int y) {

  int z;
  char buff[10];
  ...
  gets(buff);
  ...
  return;
}
```

0x00000000

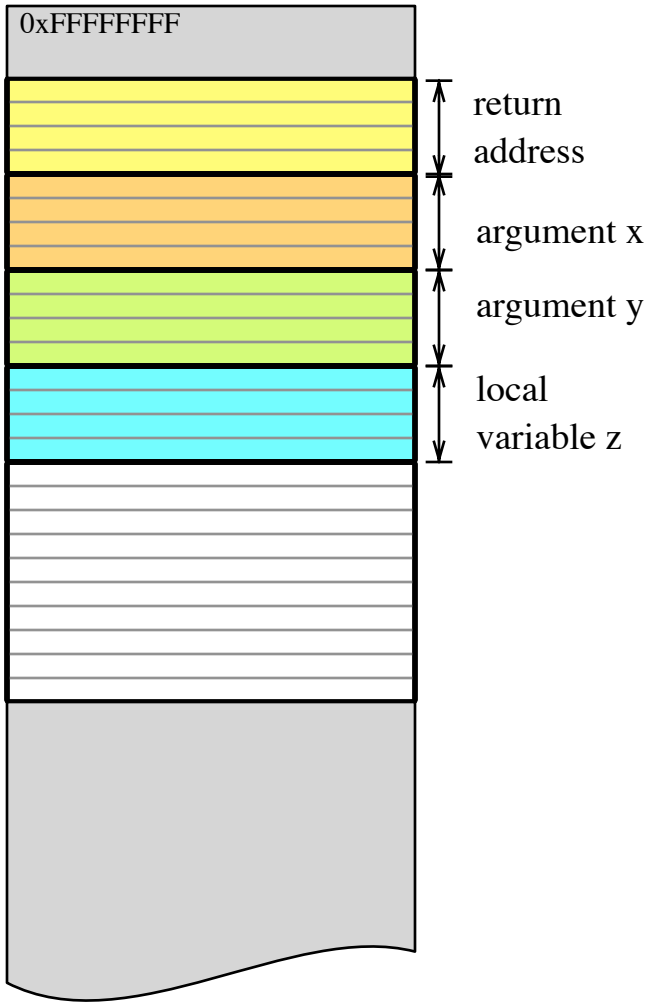
Buffer Overflow



```
main() {
  ...
  foo(12,23);
  something else;
  ...
}


foo(int x, int y) {

  int z;
  char buff[10];
  ...
  gets(buff);
  ...
  return;
}
```

0x00000000

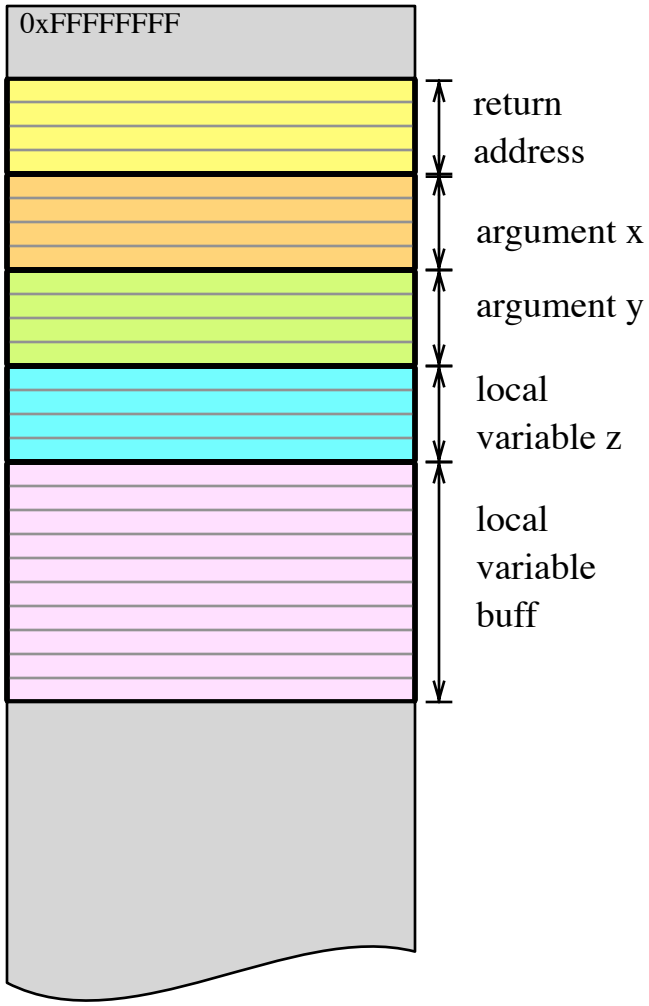
Buffer Overflow



```
main() {
  ...
  foo(12,23);
  something else;
  ...
}


foo(int x, int y) {

  int z;
  char buff[10];
  ...
  gets(buff);
  ...
  return;
}
```

0x00000000

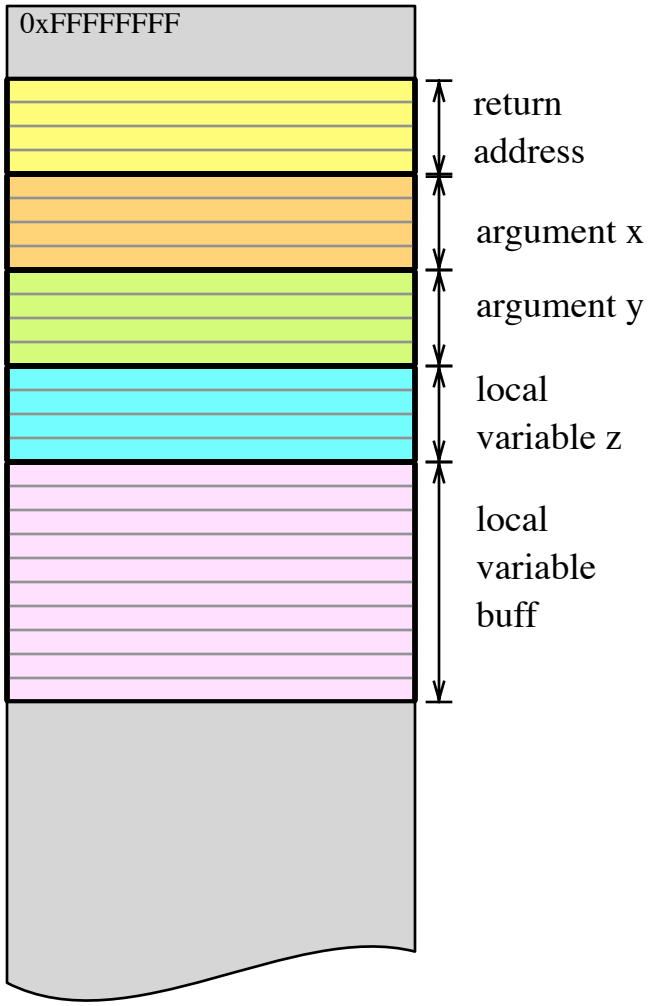
Buffer Overflow



```
main() {
  ...
  foo(12,23);
  something else;
  ...
}


foo(int x, int y) {

  int z;
  char buff[10];
  ...
  gets(buff);
  ...
  return;
}
```

0x00000000

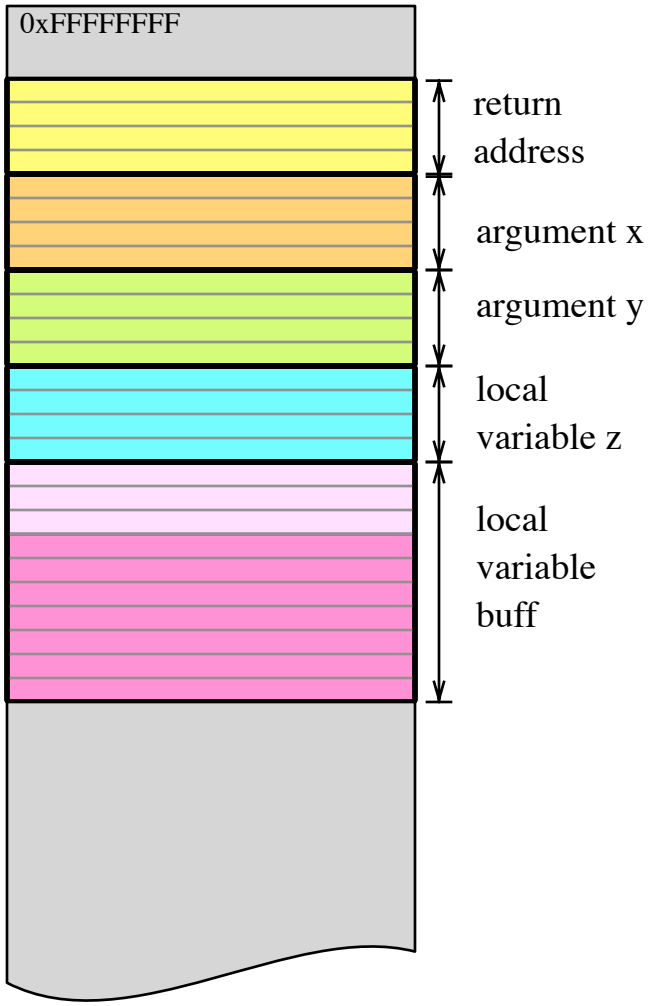
Buffer Overflow



```
main() {
  ...
  foo(12,23);
  something else;
  ...
}


foo(int x, int y) {

  int z;
  char buff[10];
  ...
  gets(buff);
  ...
  return;
}
```

0x00000000

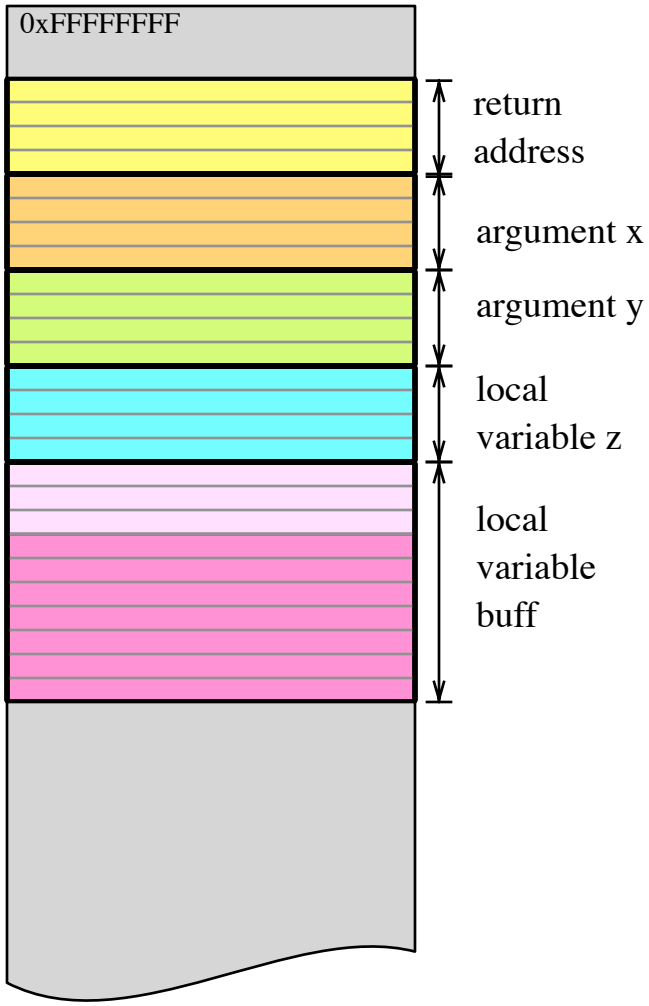
Buffer Overflow



```
main() {
  ...
  foo(12,23);
  something else;
  ...
}


foo(int x, int y) {

  int z;
  char buff[10];
  ...
  gets(buff);
  ...
  return;
}
```

0x00000000

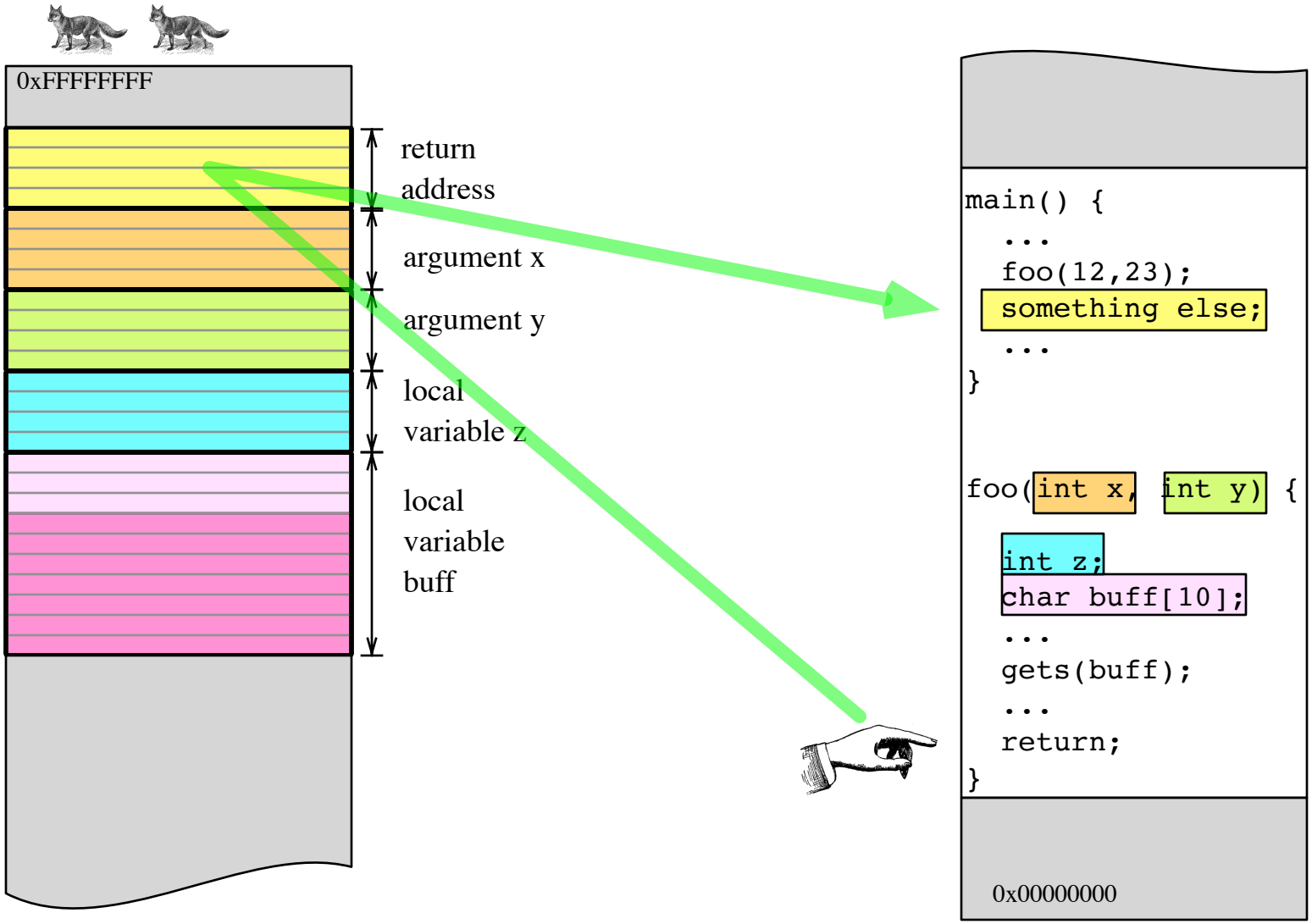
Buffer Overflow



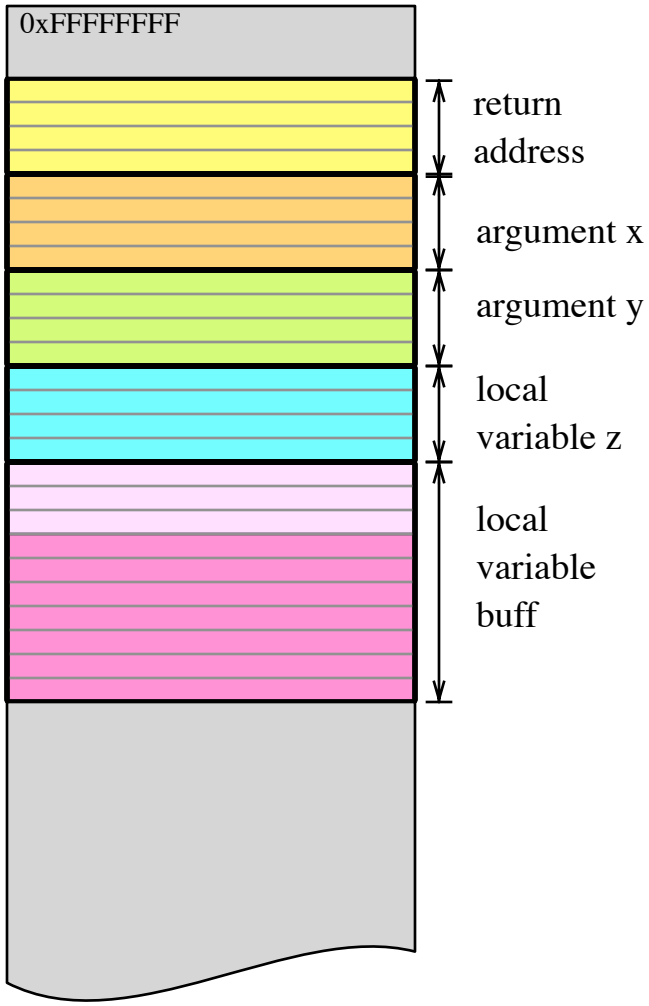
```
main() {
  ...
  foo(12,23);
  something else;
  ...
}


foo(int x, int y) {

  int z;
  char buff[10];
  ...
  gets(buff);
  ...
  return;
}
```

0x00000000

Buffer Overflow



Buffer Overflow

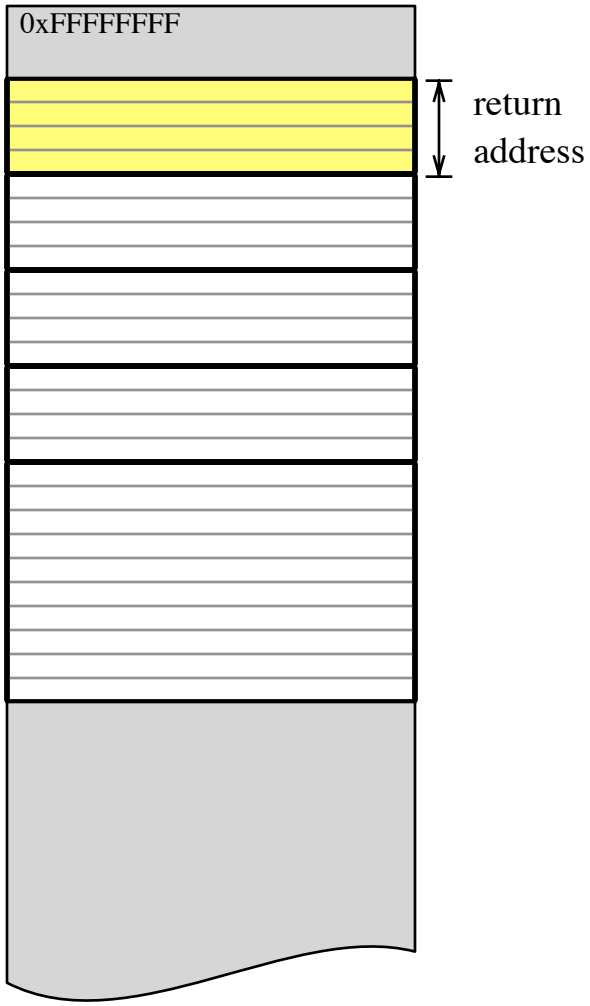


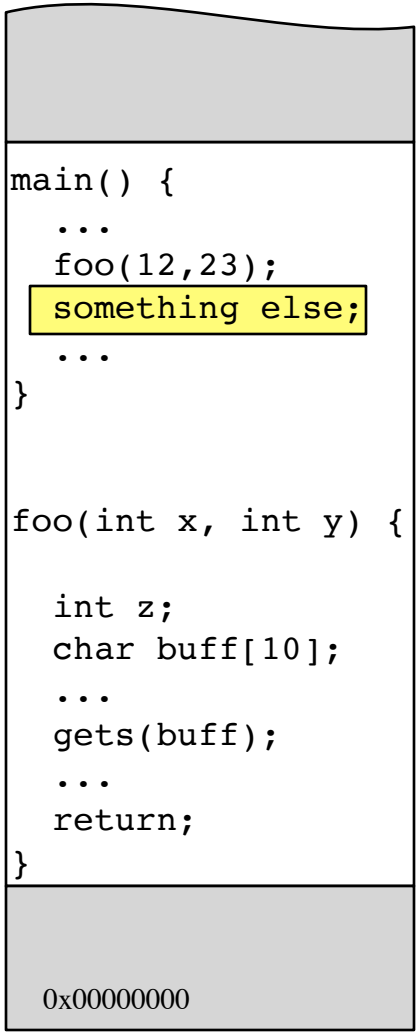
```
main() {
  ...
  foo(12,23);
  something else;
  ...
}


foo(int x, int y) {

  int z;
  char buff[10];
  ...
  gets(buff);
  ...
  return;
}
```

0x00000000

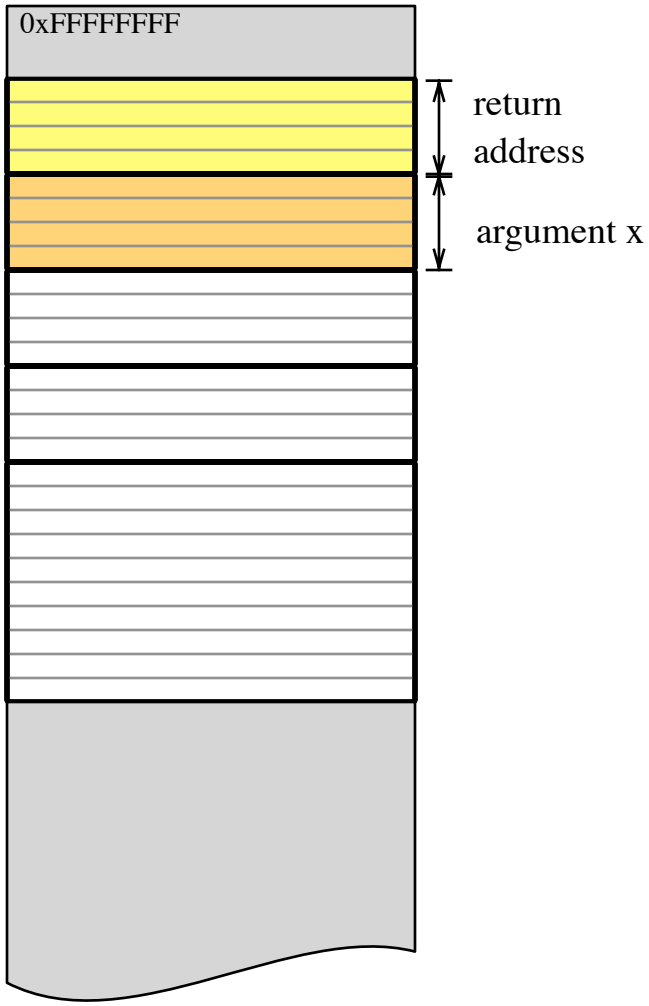
Rewind and try again!

Buffer Overflow





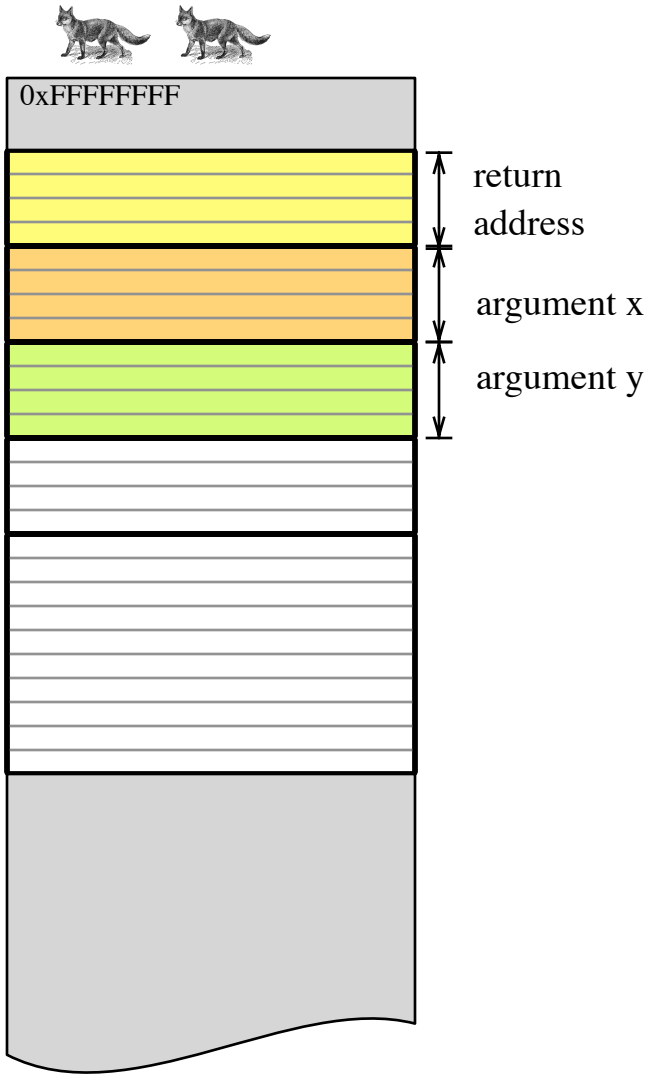
Buffer Overflow



```
main() {
  ...
  foo(12,23);
  something else;
  ...
}


foo(int x, int y) {

  int z;
  char buff[10];
  ...
  gets(buff);
  ...
  return;
}
```

0x00000000

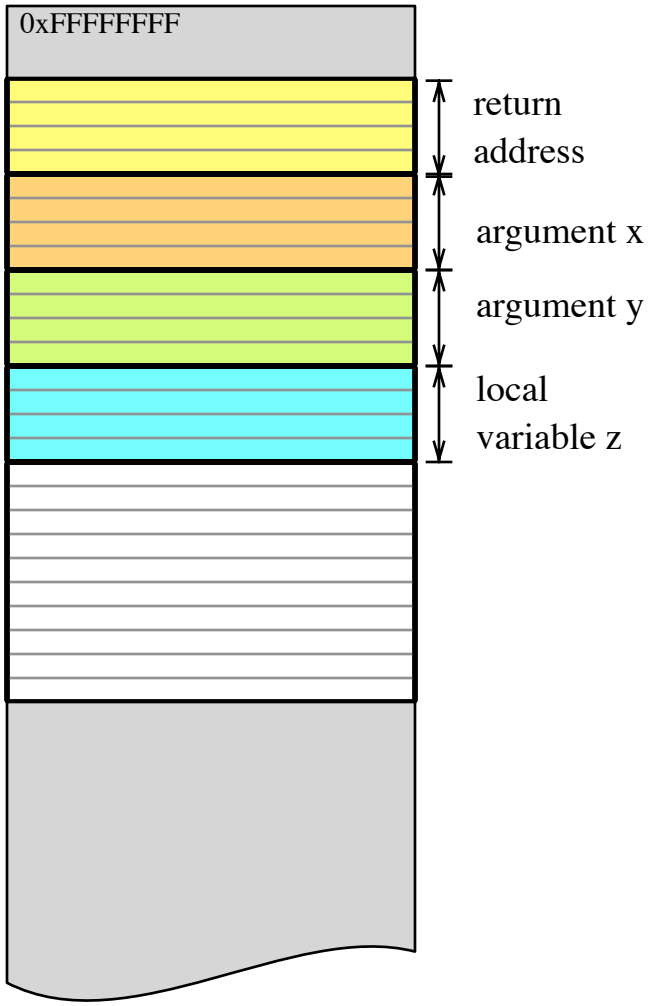
Buffer Overflow



```
main() {
  ...
  foo(12,23);
  something else;
  ...
}


foo(int x, int y) {

  int z;
  char buff[10];
  ...
  gets(buff);
  ...
  return;
}
```

0x00000000

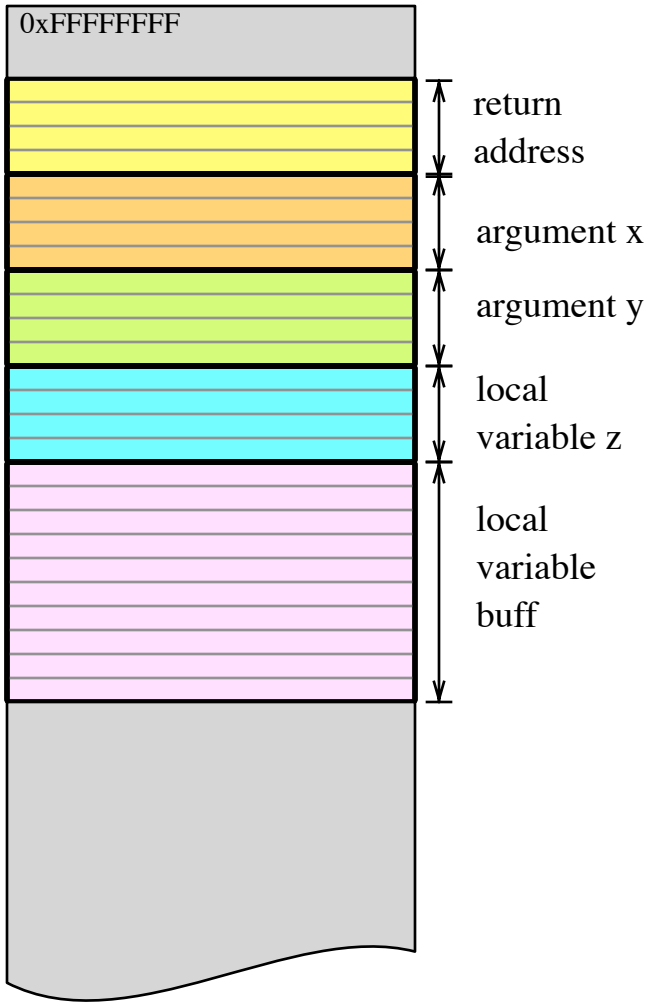
Buffer Overflow



```
main() {
  ...
  foo(12,23);
  something else;
  ...
}


foo(int x, int y) {

  int z;
  char buff[10];
  ...
  gets(buff);
  ...
  return;
}
```

0x00000000

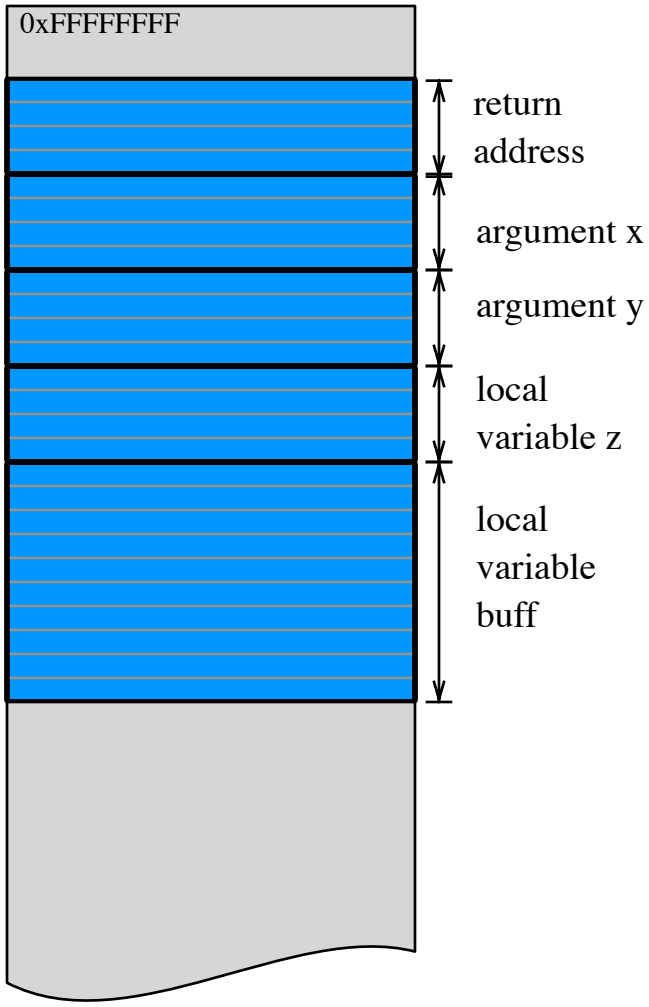
Buffer Overflow



```
main() {
  ...
  foo(12,23);
  something else;
  ...
}


foo(int x, int y) {

  int z;
  char buff[10];
  ...
  gets(buff);
  ...
  return;
}
```

0x00000000

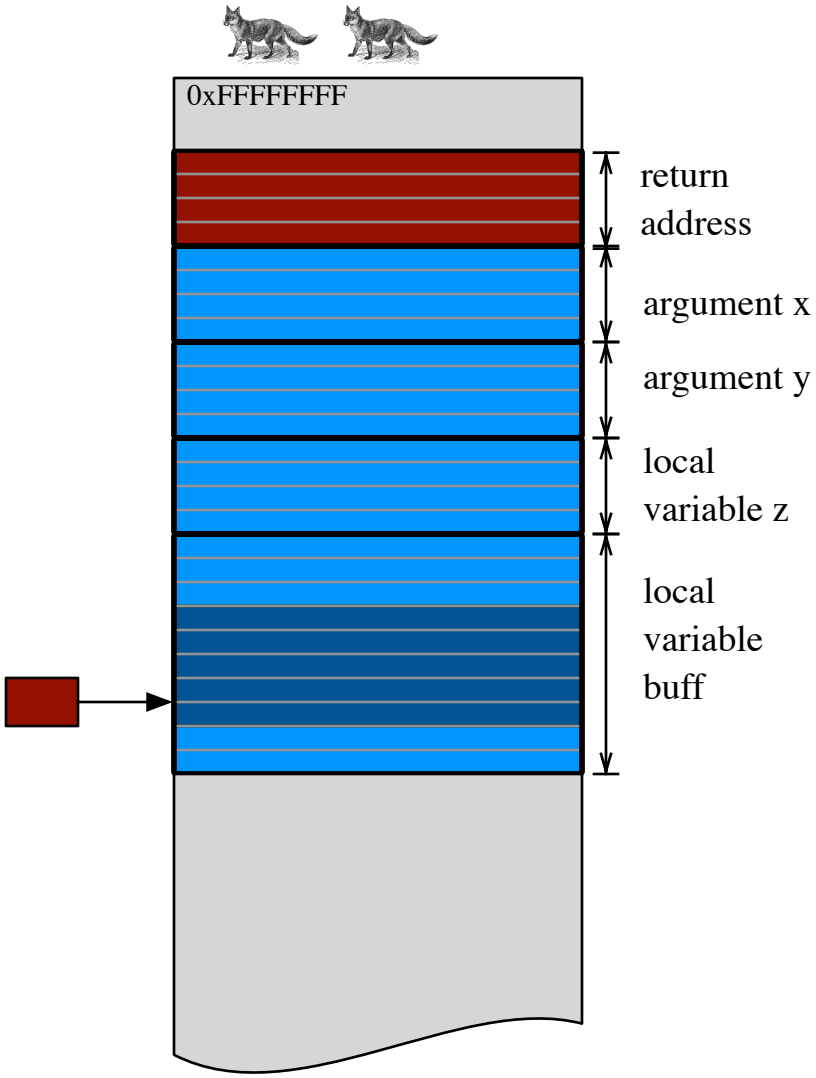
Buffer Overflow

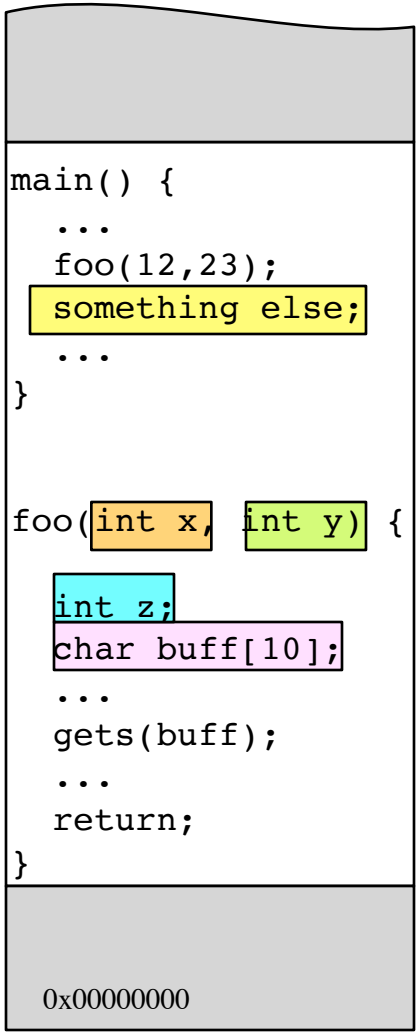


```
main() {
  ...
  foo(12,23);
  something else;
  ...
}


foo(int x, int y) {

  int z;
  char buff[10];
  ...
  gets(buff);
  ...
  return;
}
```

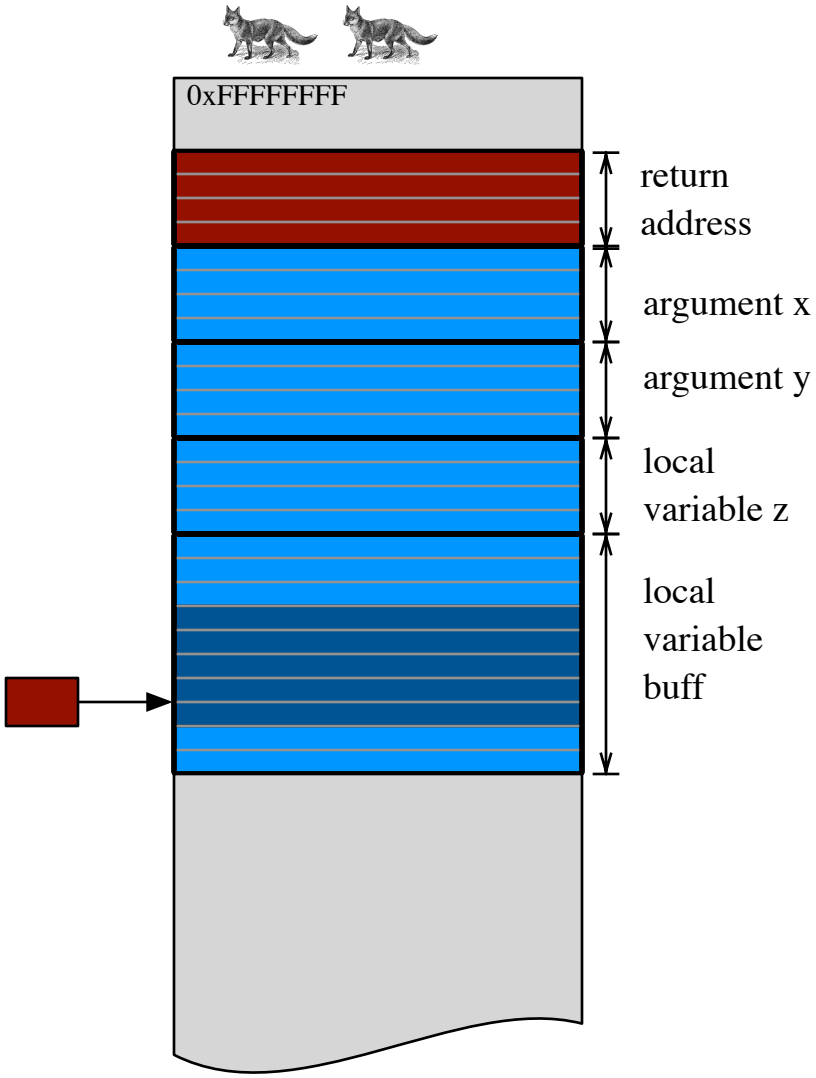
0x00000000

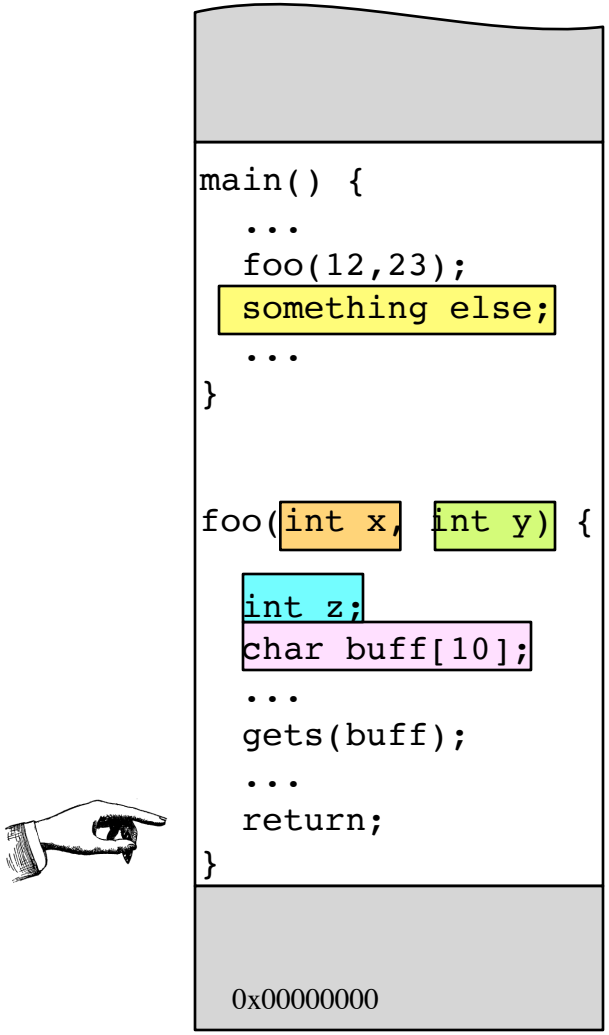
Buffer Overflow



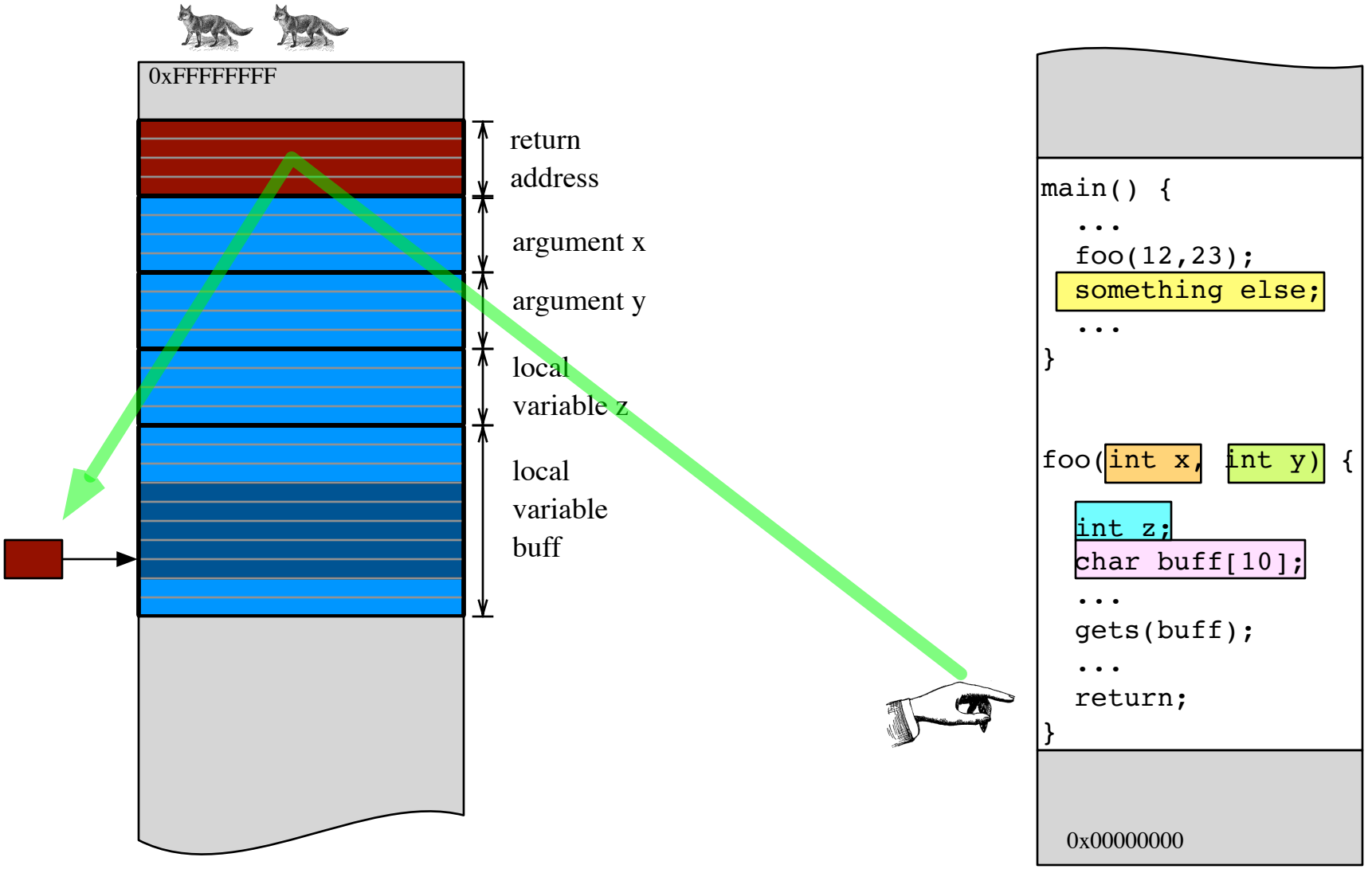


Buffer Overflow

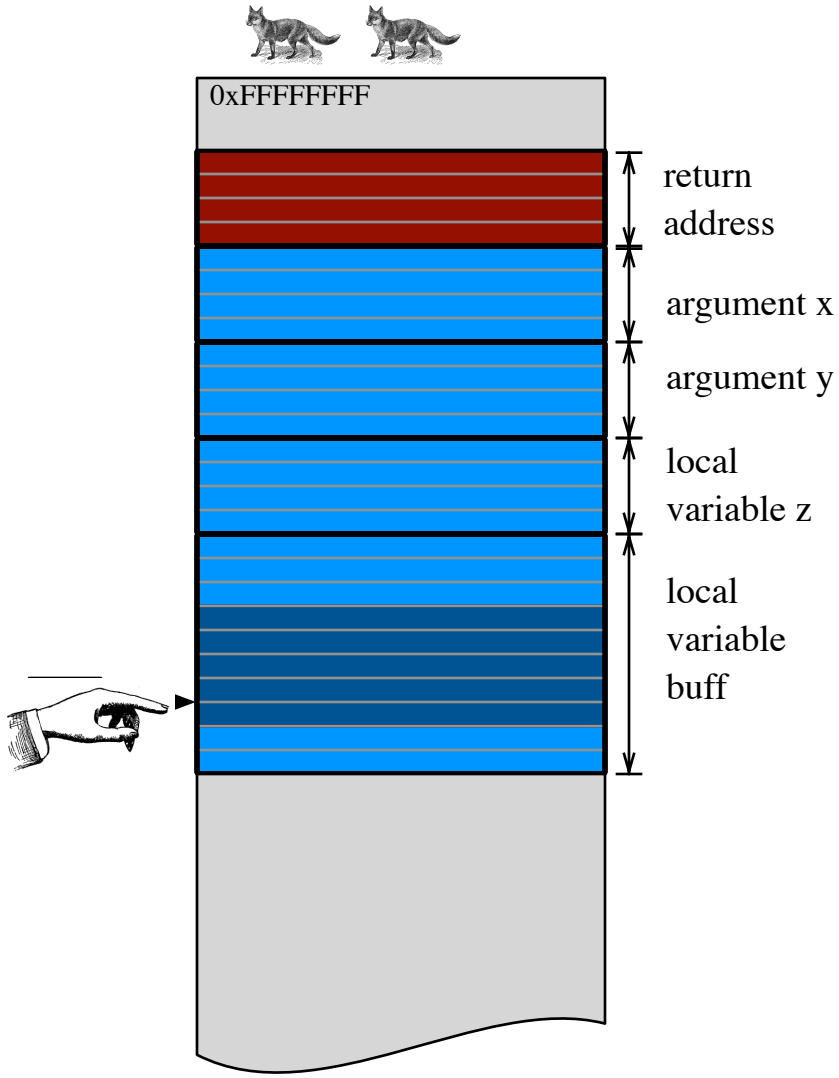




Buffer Overflow



Buffer Overflow




```
main() {
  ...
  foo(12,23);
  something else;
  ...
}


foo(int x, int y) {

  int z;
  char buff[10];
  ...
  gets(buff);
  ...
  return;
}
```

0x00000000