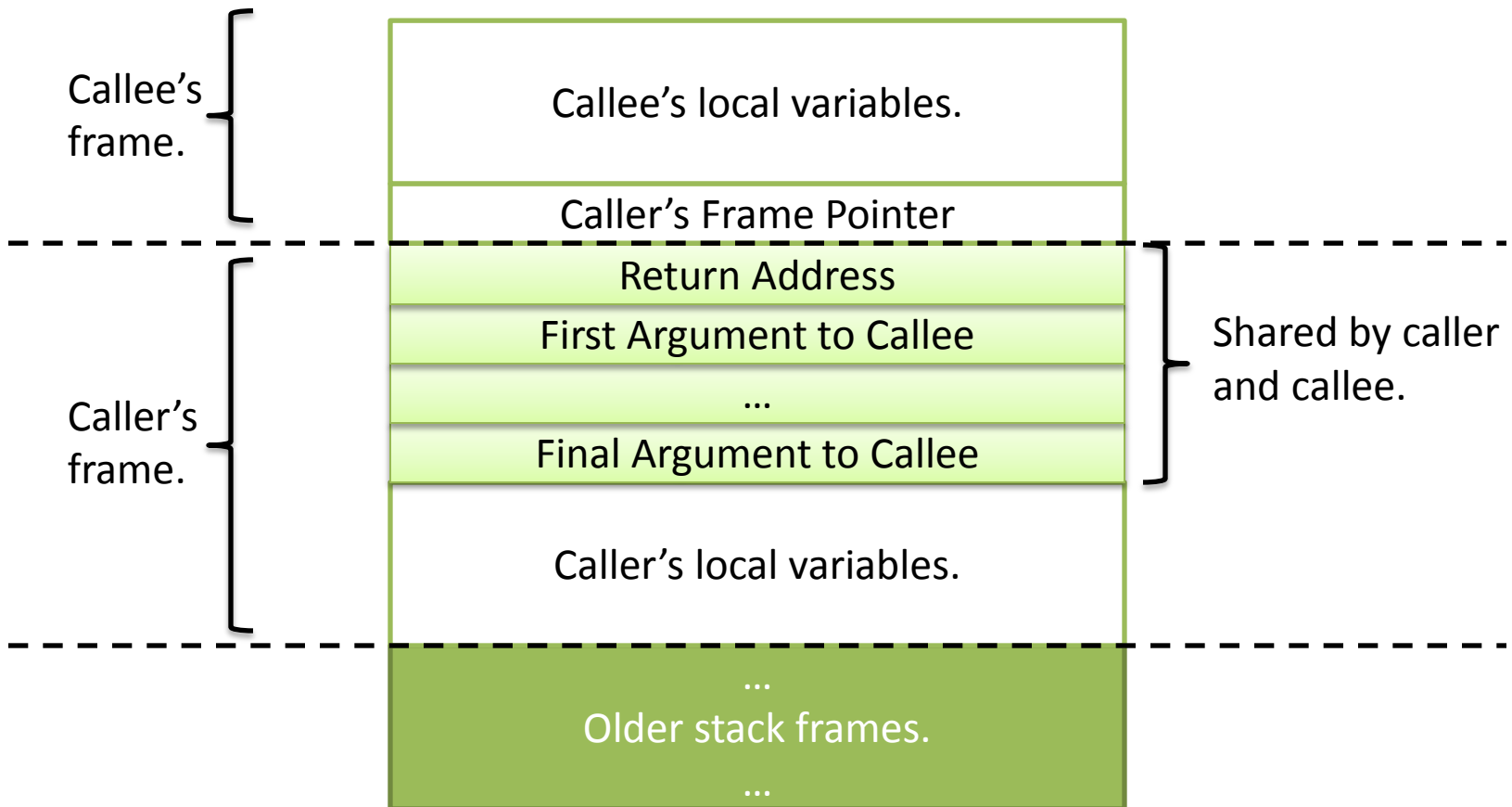


# Buffer Overflows

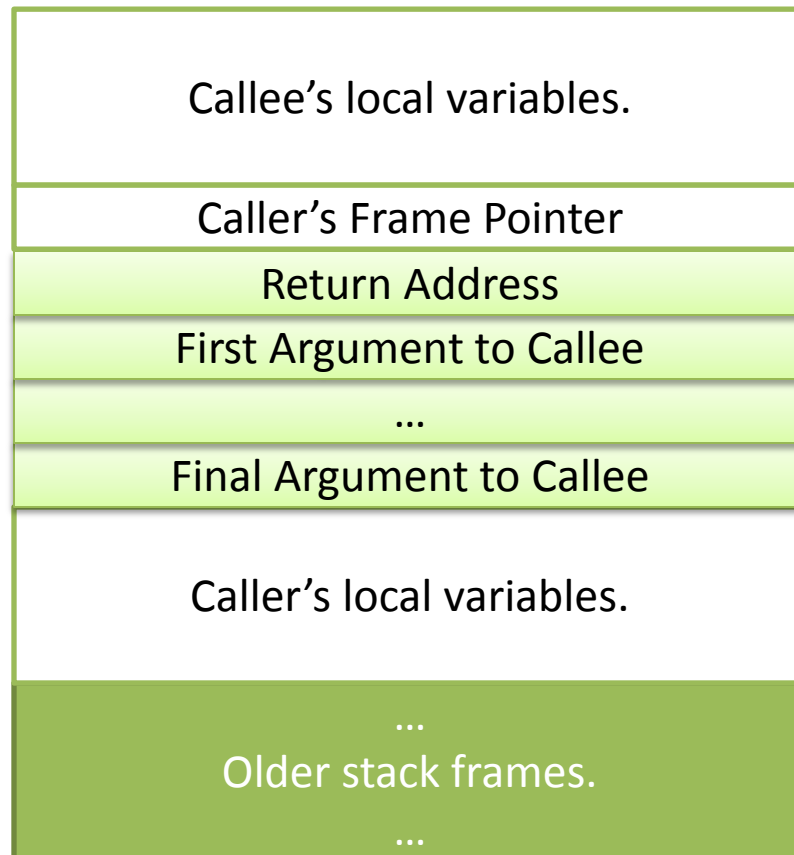
# Classic Security Vulnerability

- “Smashing The Stack For Fun And Profit”



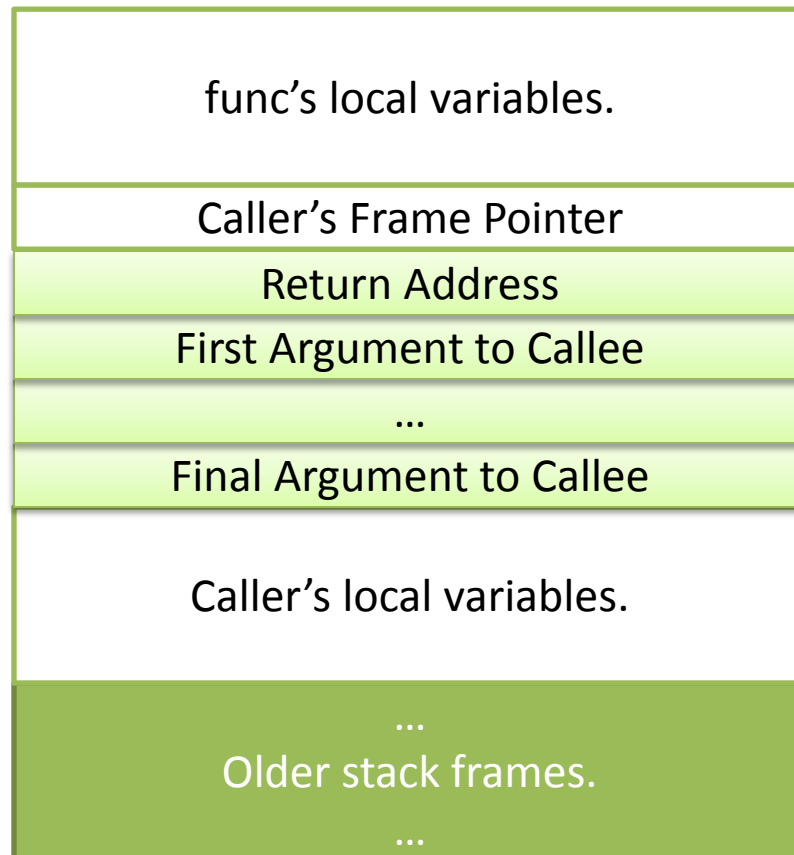
# Classic Security Vulnerability

```
void func(char *user_input) {  
    char name[100];  
    ...  
}
```



# Classic Security Vulnerability

```
void func(char *user_input) {  
    char name[100];  
    ...  
}
```



# Classic Security Vulnerability

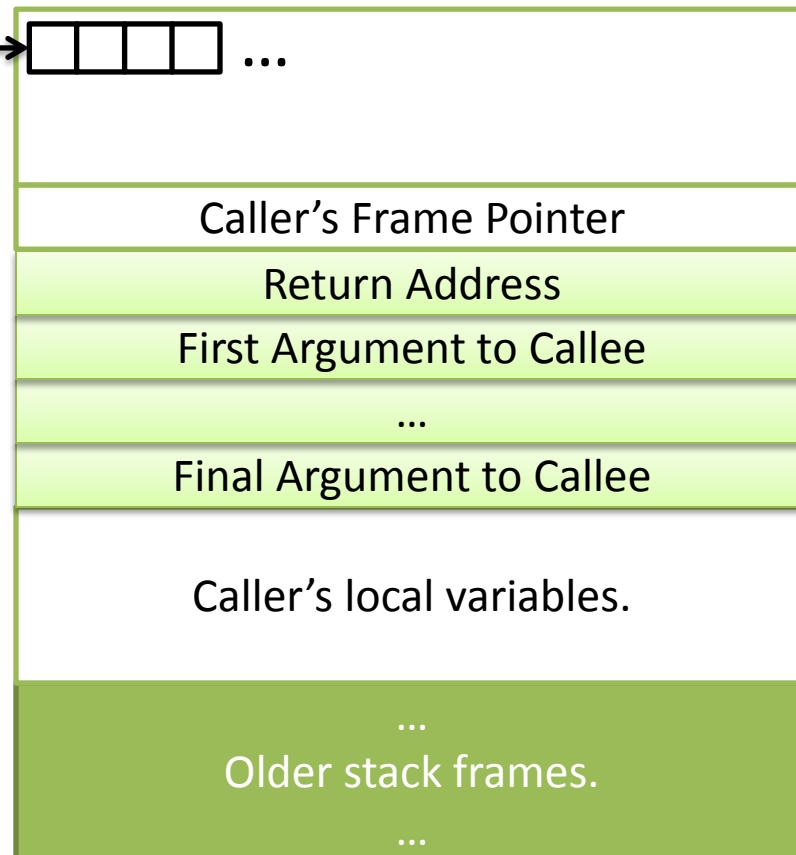
```
void func(char *user_input) {  
    char name[100];  
    ...  
}
```

name: → 

Suppose we asked a user to input their name. Is it safe to copy that into our “name” char array?

Why or why not?

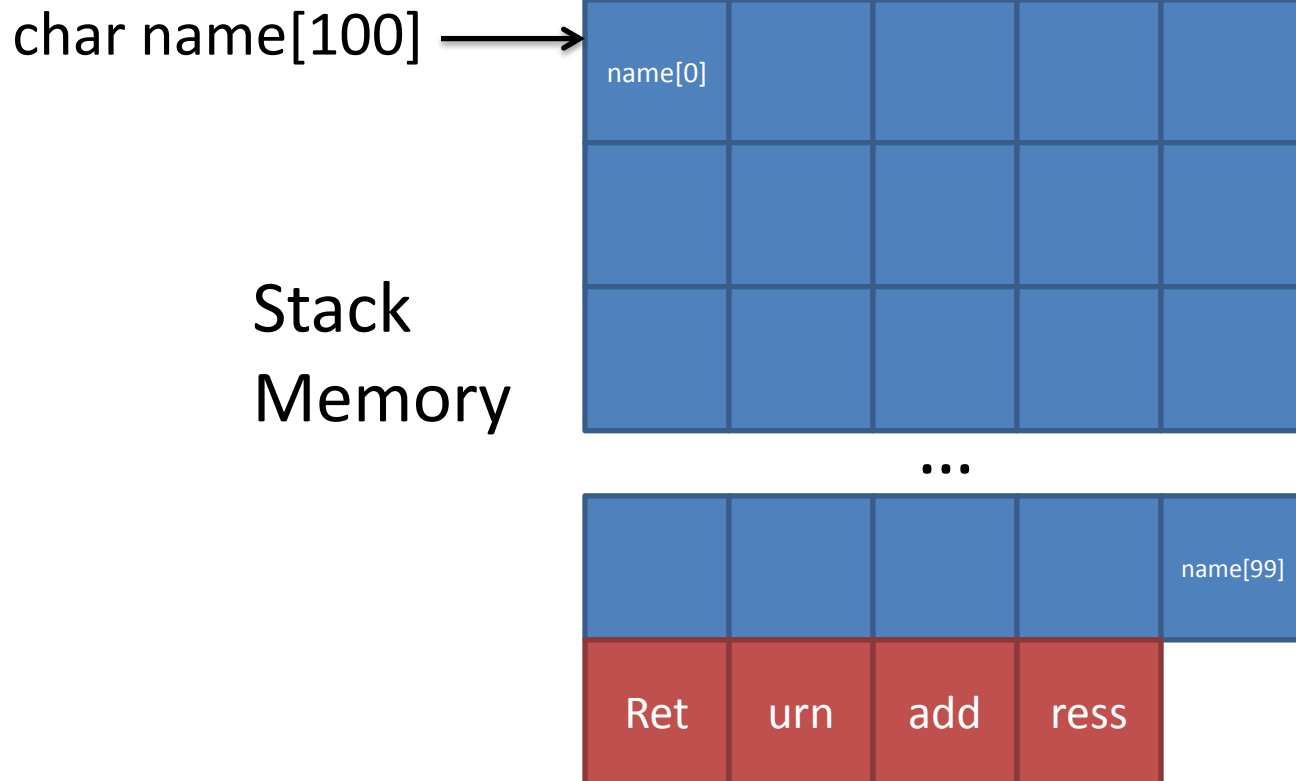
- A. Safe
- B. Not safe



# Is it safe? It depends...

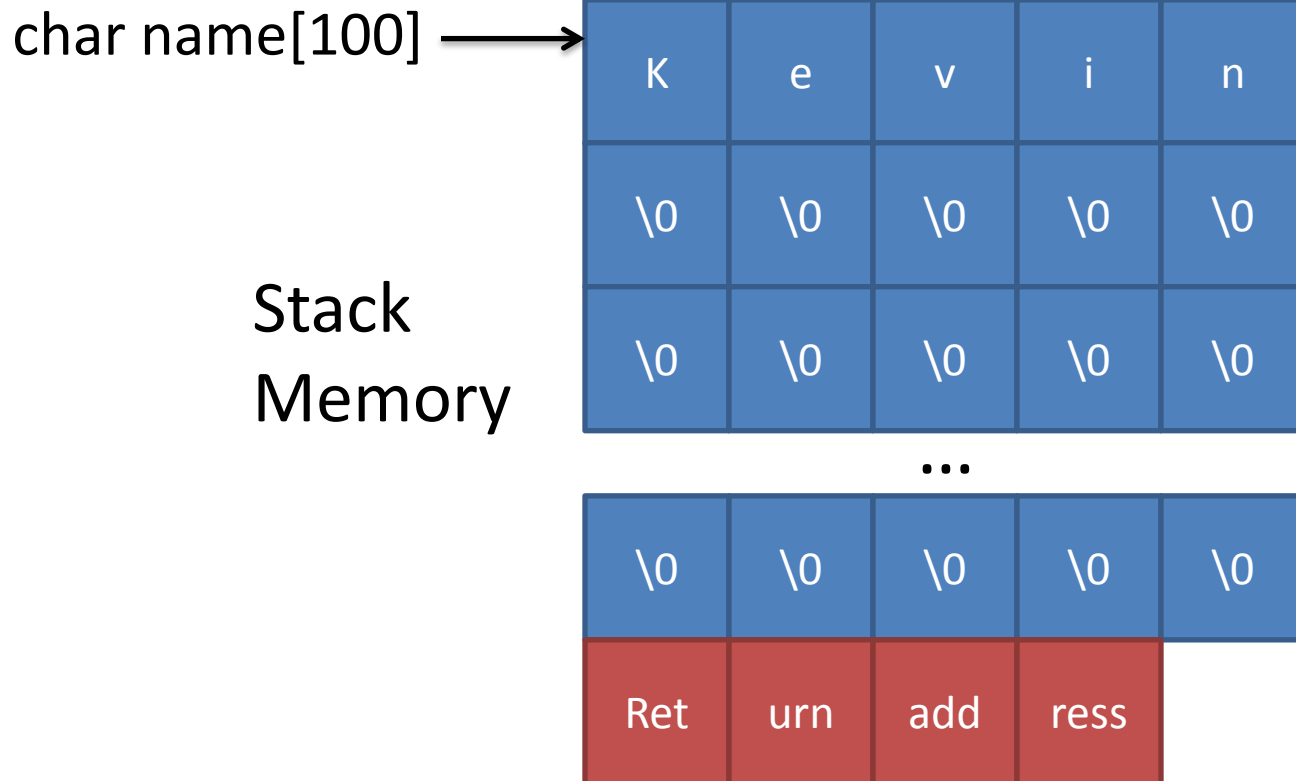
- What function are we using to do the copy?
  - strcpy? When does it stop copying?
- What happens if we copy too much?
  - Does C ensure that we don't go beyond the buffer?
  - Does strcpy?
  - What will we overwrite?
- Can we take advantage of that behavior?

# A well intentioned program...



# A well intentioned program...

If used properly, with a reasonable name, no problem here.

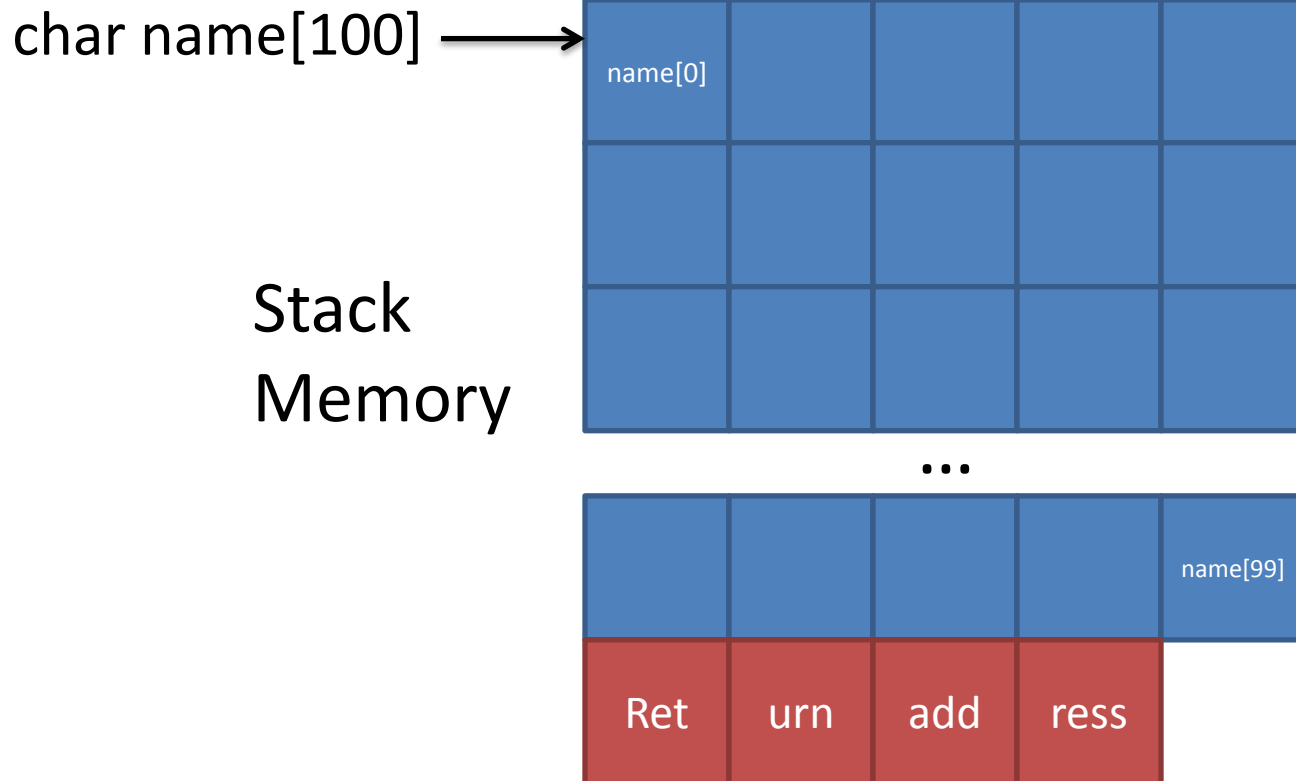




# A well intentioned program...

What if my cat steps on the keyboard and types in a name of:

asdfweffewaewerrr3f322frtfgfgdfgrgrdgrgdgvcdllliuiyytylj;jouiyiytytrf  
bbncbvcxcxzv,mn.,n.,mloiuytytytgjkghgfgfdtreyteretdgfhdfsdfsds

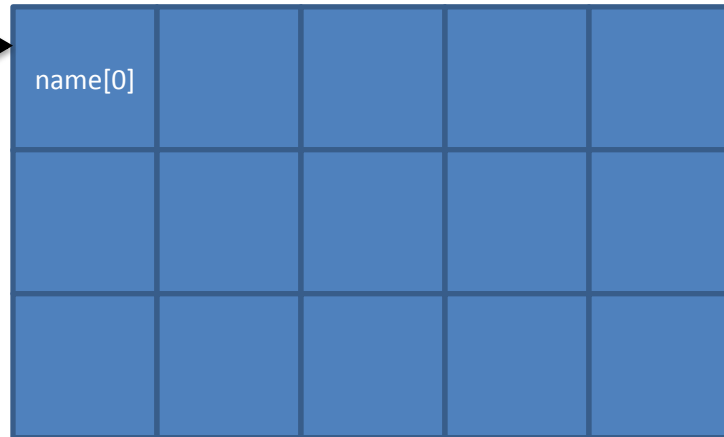


# A well intentioned program...

What if my cat steps on the keyboard and types in a name of:

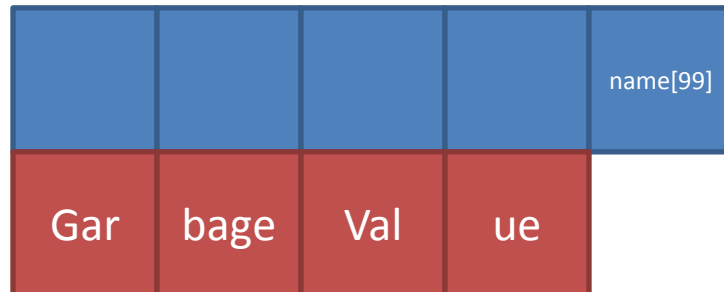
asdfweffewaewerrr3f322frtfgfgdfgrgrdgrgdgvcdllliuiyytylj;jouiyiytytrf  
bbncbvcxcxzv,mn.,n.,mloiuytytytgjkghgfgfdtreysteretdgfhdfjfsdfsds

char name[100]



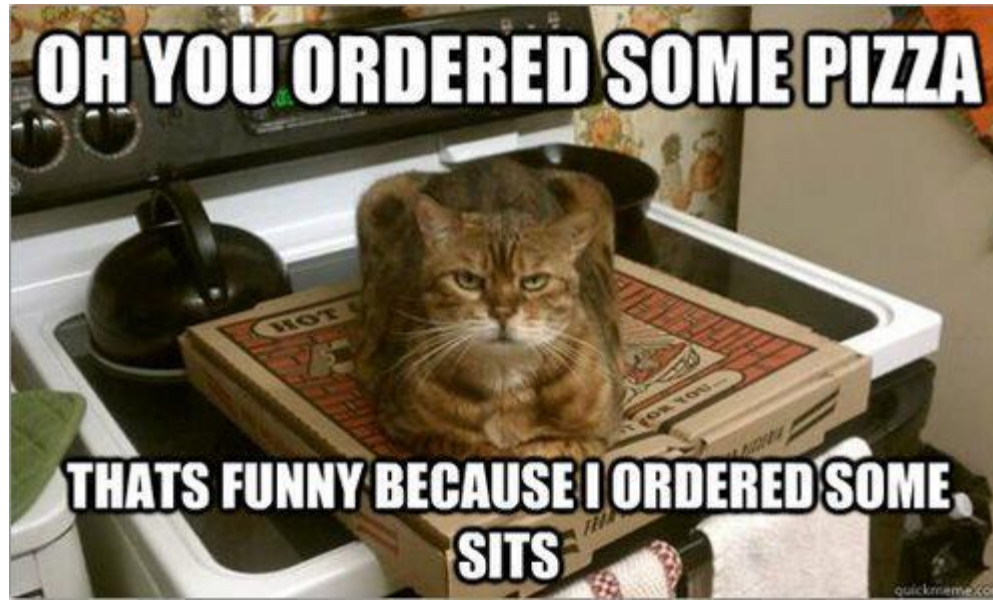
Stack  
Memory

...



Set PC to this  
value on return!  
What'll happen?





Cat, performing the classic “Denial of Pizza” attack.

- Is crashing the program the worst we can do?

# A well intentioned program...

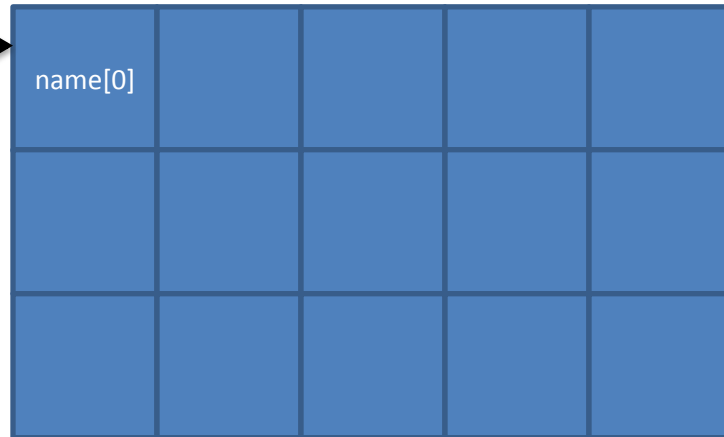
Suppose I want to change the return address to do Evil™

Fake\_name\_that's\_really\_long\_to\_fill\_100\_characters\_\_\_\_\_...\_\_\_\_\_0xFE327

---

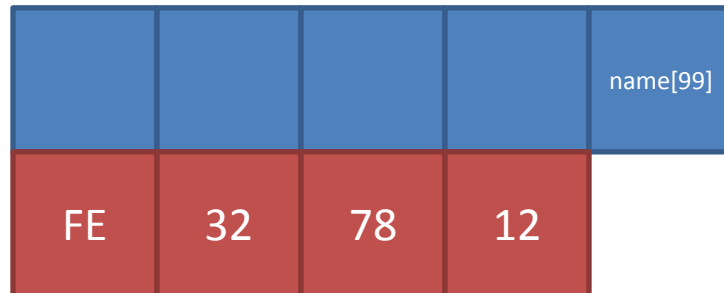


char name[100]

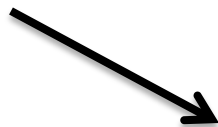


Stack  
Memory

...



Set PC to this  
value on return!  
What'll happen?

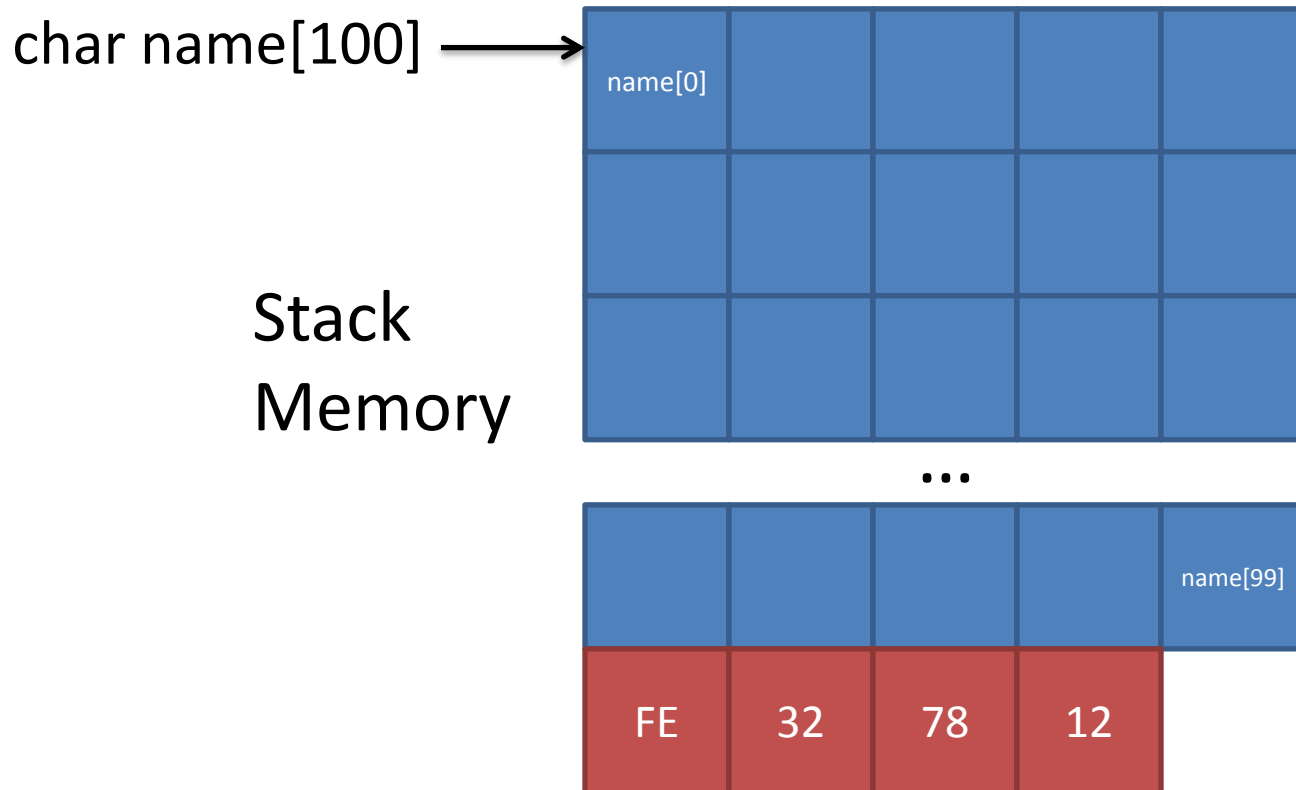


Does this help me  
be evil?

# A well intentioned program...

If I can set the return address to be an arbitrary pointer, I can control what gets executed next!

If only I could add my own instructions in memory somewhere...

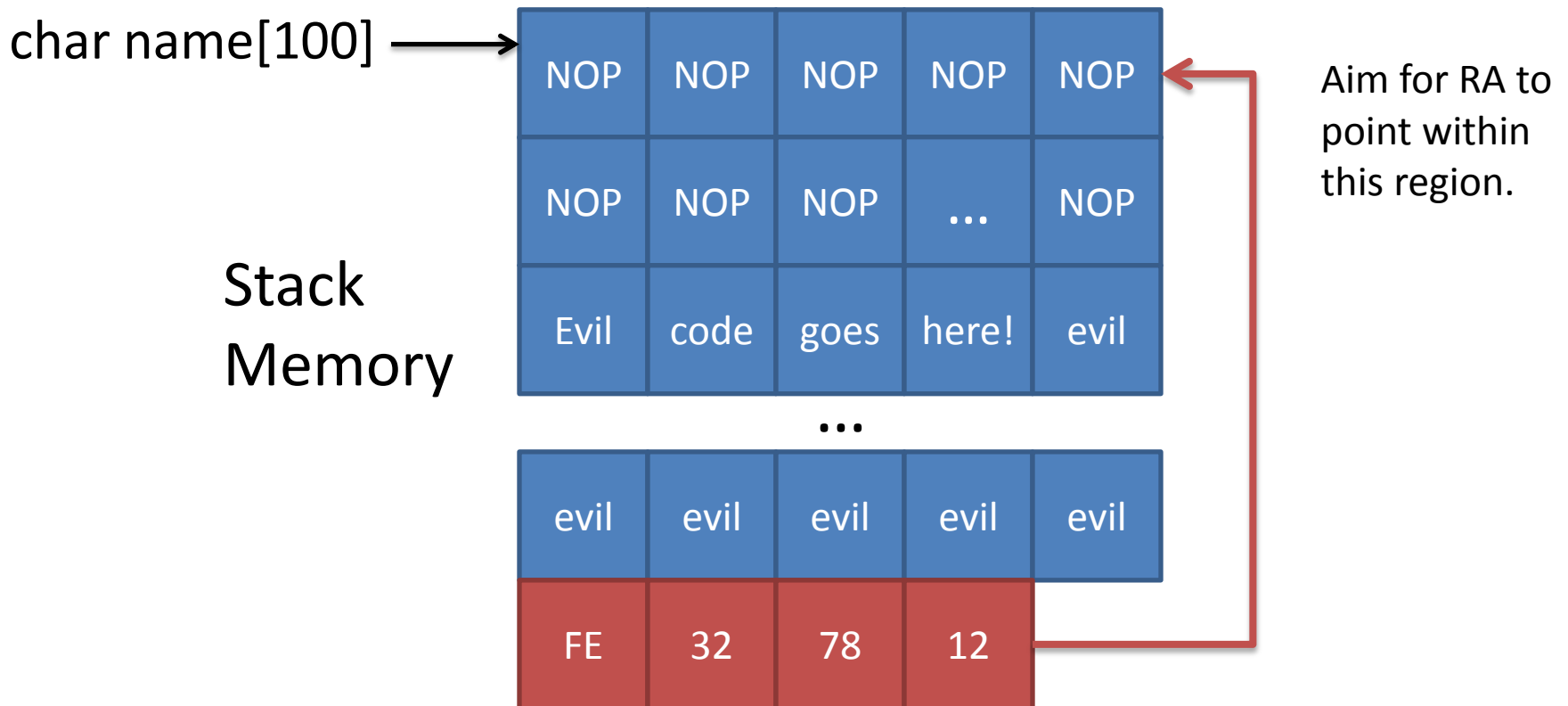


# A well intentioned program...

Suppose I want to change the return address to do Evil™

[Do nothing (NOP)]...[Do nothing (NOP)]

[Evil™ Code that sends all your secrets to me]0xFE327812



One careless strcat . . . Yours ?



*Remember*—Only you can  
**PREVENT BUFFER OVERFLOWS !**

U. S. Department of Agriculture  
Forest Service

SMOKE AND POLLUTIONS KILL THE WILDLIFE  
PROTECTED BY A PUBLIC SERVICE OF FOREST SERVICE  
A COMMUNITY PROGRAM

U.S. Forest Department