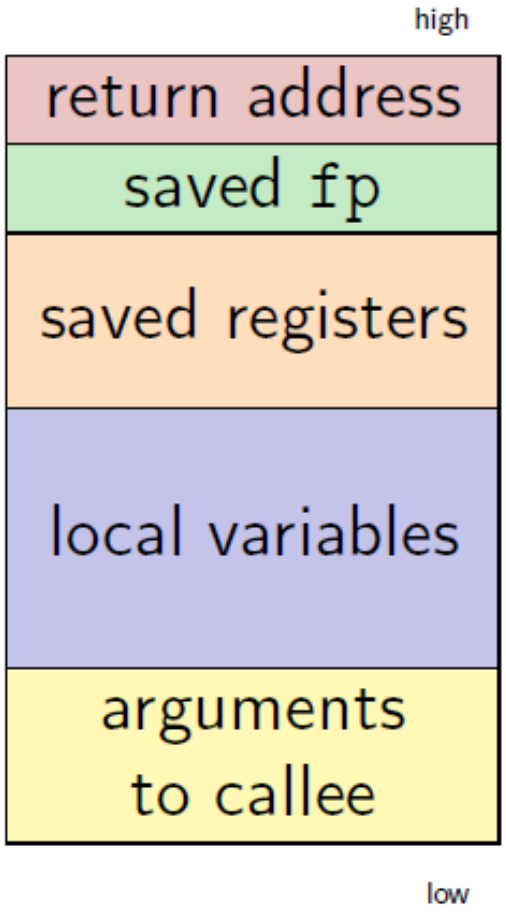
Stack buffer overflow

Stack frame layout

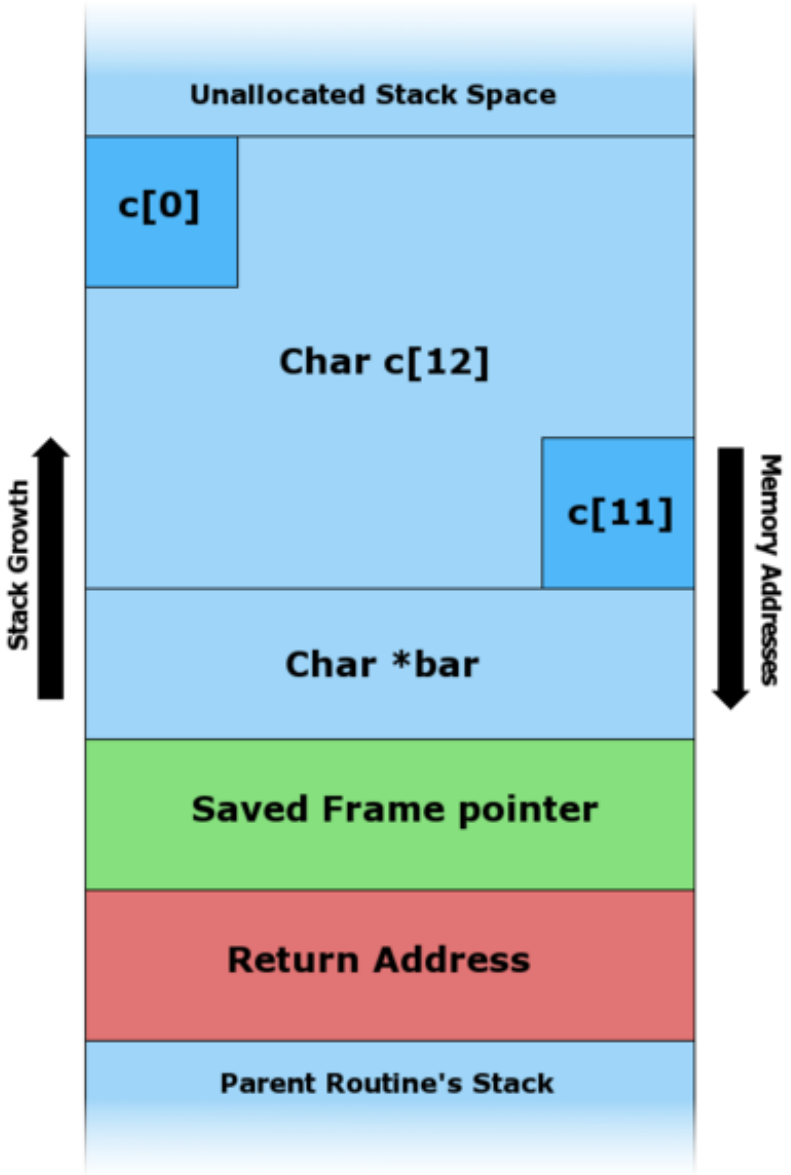


```
#include <string.h>

void foo (char *bar)
{
   char c[12];
   strcpy (c, bar); //no bound
}

int main (int argc, char **argv)
{
   foo(argv[1]);

}
```

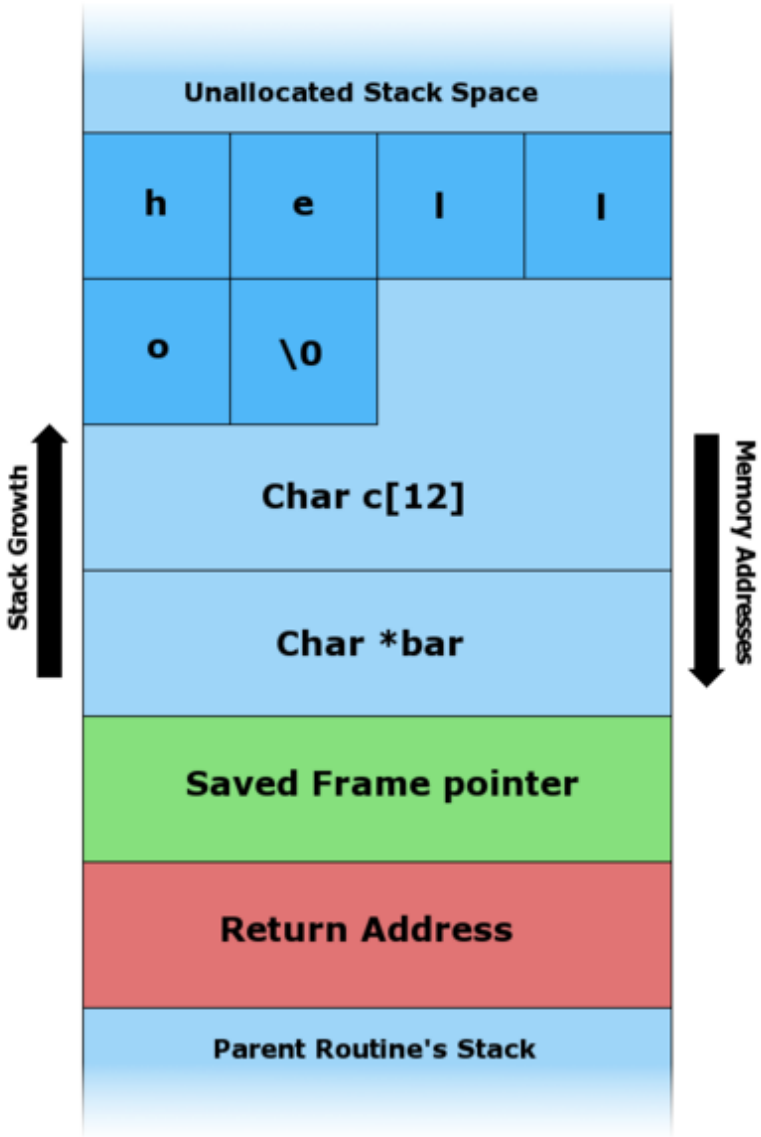


```
#include <string.h>

void foo (char *bar)
{
   char c[12];
   strcpy (c, bar); //no bound
}

int main (int argc, char **argv)
{
   foo(argv[1]);

}
```

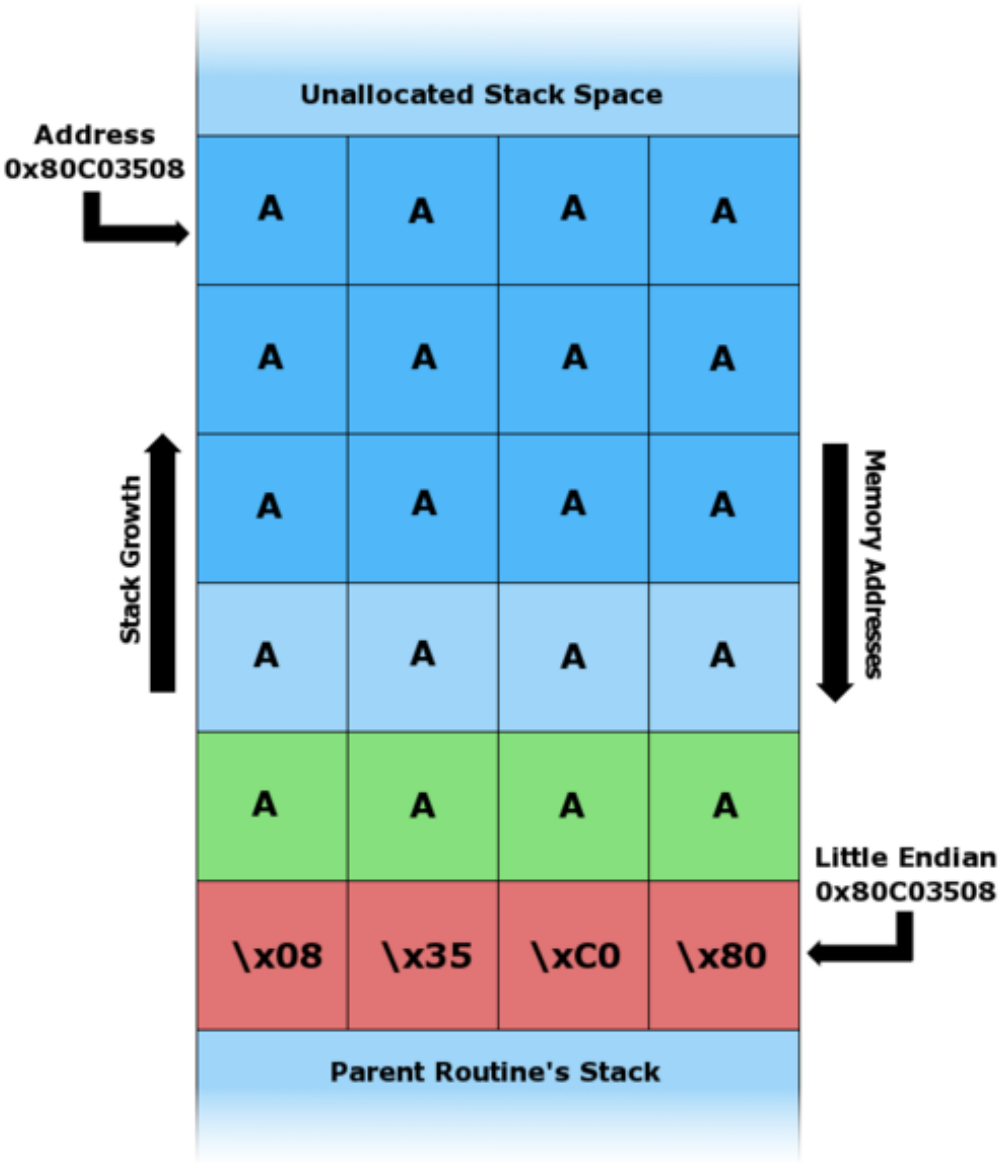


```
#include <string.h>

void foo (char *bar)
{
   char c[12];
   strcpy (c, bar); //no bound
}

int main (int argc, char **argv)
{
   foo(argv[1]);

}
```



Demo

- Linux

Homework 3

- Due next week. Tuesday??
- Stack buffer overflow problem, very similar to what we have described today.
- Demo.

Linker Exercise

- 2.31