1 Unix, C und Sicherheit

- Beispiel-Lösung eines Studenten von Aufgabe 6 (ryash)

```
int main (int argc, char *argv[])
{
    char password[maxArgsLength+1];

    ... /* socket oeffnen und stdin umleiten */

    scanf ("%s", password);

    ...
}
```

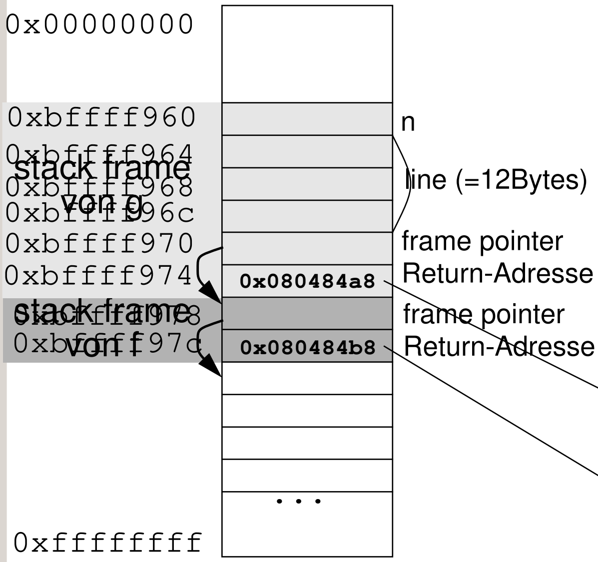

2 Ausnutzen des Pufferüberlaufs

- Häufiges Problem: Puffergrößen sind nicht ausreichend
  - Beispiel scanf - Linux,x86 (Wortgröße = 32 Bit)

```
#define MAXLINE 12
char line[MAX_LINE];
int n;
n = scanf("%s", line);
```

  - Eingabe von "`0123456789ab`" + `0x00000000` + `0xbffff978` + code
  - Beispiel für code: `execl("/bin/sh", "/bin/sh", 0);`

3 Stack Layout (Linux, x86)




```
#include <stdio.h>

void g() {
  char line[12];
  int n;
  n = scanf("%s", line);
}

void f() {
  g();
}

int main(int argc, char *argv[]) {
  f();
}
```


3 Vermeidung von Puffer-Überlauf

- scanf
  - char buf[10]; scanf("%9s", buf);
- gets
  - Verwendung von fgets
- strcpy,strcat
  - Überprüfung der String-Länge oder
  - Verwendung von strncpy, strncat
- sprintf
  - Verwendung von snprintf