Buffer Overflows

Valentin Brandl <mail@vbrandl.net>

Fakultät Informatik und Mathematik

20. September 2022

Inhalt

- Maschinennahe Programmiersprachen ohne Memorysafety (z.B. C, C++, Assembly, FORTRAN) erlauben es, Speicher beliebig zu beschreiben
- Bei fehlender Validierung kann ein Programm mehr Speicher schreiben, als eigentlich reserviert wurde und dabei andere Daten im RAM überschreiben
- Entsprechend präparierter Input kann dazu führen, dass ein Angreifer den Ablauf der Programmausführung übernehmen kann

```c
#include<stdio.h>
#include<string.h>
void foo(char *input) {
  char buf[50];
  strcpy(buf, input);
  puts(buf);
}
int main(int argc, char **argv) {
  foo(argv[1]);
}
```