Razhroščevalnik

Seminarska naloga pri predmetu Sistemska programska oprema
Mentor: doc. Tomaž Dobravec

Jan Mrak
Fakulteta za računalništvo in informatiko, Univerza v Ljubljani

13. januar 2025

Povzetek

Predstavitev implementacije in delovanja rezhroščevalnika na različnih platformah in za različne jezike.

1 Uvod

Razhroščevalnik je program, ki nam omogoča testiranje in upravljanje nekega drugega programa. Omogoča nam branje in pisanje spomina in registrov, poljubno ustavljanje programa, izvajanje po vrsticah ali ukazih in drugo. Poznamo različne razhroščevalnike, kot so GDB, LLDB, x64dbg, …

2 Razhroščevalnik na sistemu Linux

Na Unix in Unix-like sistemih je priskrbljen sistemski klic

```
long ptrace(enum __ptrace_request op, pid_t pid, void *addr, void *data);
```

, ki nam omogoča, da lahko dostopamo do prcesa podanega s `pid`. Da pa bo sistemski klic uspel, mora proces, do katerega želimo dostopati, dovoliti dostop do njega. To pa lahko naredi s klicem sistemske funkcije `ptrace`:

```
// pid, addr in data argumenti so ignorirani
ptrace(PTRACE_TRACEME, 0, NULL, NULL);
```

Po tem bo razhroščevalnik lahko dostopal do tega procesa.

Razhroščevalnik lahko sam ustvari proces, ki potem pokliče `ptrace` z argumentom `PTRACE_TRACEME`,

```
int pid = fork();
if (pid == 0) {
    ptrace(PTRACE_TRACEME, 0, NULL, NULL);
    execve(...);
}
```

lahko pa se priklopi na nek obstoječi proces z uporabo `PTRACE_ATTACH`, ki pošlje signal `SIGSTOP`, da se proces ustavi, ali pa `PTRACE_SEIZE`, ki ne ustavi procesa.

```
ptrace(PTRACE_ATTACH, pid, NULL, NULL);
// ali
ptrace(PTRACE_SEIZE, pid, NULL, PTRACE_O_flags);
```

3 Razhroščevalnik na sistemu Windows

4 Razhroščevalnik za jezik Java / Python ?