MAŠĪNKODA INSTRUMENTĒŠANA BLOKU IZPILDES STATISTISKAJAI ANALĪZEI UN PAREDZĒŠANAI

Kursa dara pirmajā daļā tika aprakstīti dažādi mašīnkoda apgrieztas inženierijas pielietojumi (autortiesību aizsardzība, komercnoslēpuma aizsardzība, ievainojamību meklēšana programmatūrā, pirmkoda atgūšana). Tālāk tika detalizēti aprakstīti soļi binārās analīzes veikšanai. Soļu apraksta laikā uzsverot un parādot cik svarīga ir programmas bloku izpildes noteikšana – kāda būs nākamā funkcija? Kāds būs nākošais koda lēciens? Ko šāda informācija dod binārās analīzes veicējam katrā no apgrieztās inženierijas pielietojumiem?

```
.def ___main; .scl 2; .type 32; .endef
 .section .rdata,"dr"
LC0:
 .ascii "type a word \0"
LC1:
 .ascii "%c \0"
 .text
 .globl _main
 .def _main; .scl 2; .type 32; .endef
_main:
 pushl %ebp
 movl %esp, %ebp
 andl $-16, %esp
 addl $-128, %esp
 call ___main
 movb $97, 127(%esp)
 movl $0, 120(%esp)
 movl $LC0, (%esp)
 call _puts
 jmp L2
```

Kursa darba otrajā daļā tika aplūkotas, kādas ir šobrīd pieejamas metodes binārās analīzes ātruma uzlabošanai: heiristiski rīki, atkļūdotāji, simbolu faili. Pēc apskates tika aprakstīta un piedāvāta jauna metode: bloku izpildes statistiskā analīze un paredzēšana. Veicot bloku analīzi ir iespējams paredzēt programmas darbību, atvieglojot izpēti un ātrāk iegūstot apgrieztās inženierijas pielietojuma rezultātus. Tika apskatīti arī citi šobrīd pieejami risinājumi, un tie salīdzināti ar oriģināli piedāvāto.