Arhitektura računara – Predmetni projekat

Program eit386 v2.1

Autor: Milan Stanojević Mentor: Lazar Stričević

Fakultet tehničkih nauka, Novi Sad, maj 2017.

eit386 v2.1

eit386 v2.1 je program koji injektuje novi mašinski kod u postojeći 32bitni elf izvršni fajl. Injektovani kod će se izvršiti prilikom pokretanja izvršnog fajla i nakon toga program nastavlja izvršavanje sopstvenog koda.

eit386 je skraćenica od ELF Injection Tool, 386 označava da program trenutno može da injektuje samo 32bitni mašinski kod u 32bitne ELF izvršne fajlove.

eit386 v2.1 ima dvije opcije rada a to su:

- Zaštita izvršnog fajla od izmjene tj. infekcije
- Injektovanje 32bitnog elf objekta u izvršni fajl

Zaštita izvršnog fajla

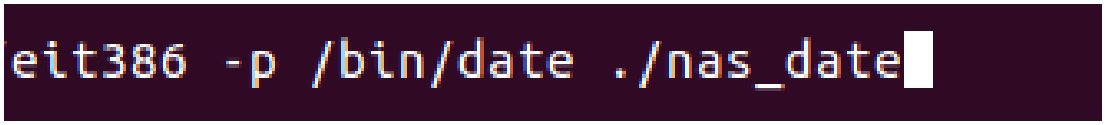
Program će injektovati zaštitni kod u izvršni fajl tako da prilikom svakog pokretanja izvršnog fajla, zaštitni kod provjerava checksum-u našeg izvršnog fajla, ako je checksum-a u redu izvršni fajl nastavlja izvršavanje sopstvenog koda, a ako se ne poklapa ispisuje poruku da je izvršni fajl zaražen.

Zaštita izvršnog fajla pokreće se ovako:

./eit386 –p input_elf new_protected_elf

input_elf je izvršni fajl koji hoćemo da zaštitimo

new_protected_elf je izvršni fajl sa ubačenom zaštitom



Injektovanje 32bitnog elf objekta u izvršni fajl

Program injektuje 32bitni kompajliran(ne linkovan) elf objekat u izvršni fajl. **Trenutno kod objekta se može pisati samo u asembleru jer je potrebno da promjenljive budu u .text sekciji da bi kod radio u izvršnom fajlu.**

Takođe asemblerski kod mora da ima labelu e_entry sa instrukcijom jmp 0xffffff, ta instrukcija će biti zamjenjena sa adresom e_entry od našeg izvršnog fajla.

Na kraju se mora skočiti na labelu e_entry, inače novi izvršni fajl neće nastaviti izvršavanje sopstvenog koda.

Primjer koda:

```
.section .text
.globl main
main:
        pusha

        movl $4, %eax
        movl $1, %ebx
        movl $msg, %ecx
        movl $12, %edx
        int $0x80

        popa
        jmp e_entry

msg:
                .ascii  "Hello world\n"
e_entry:
        jmp 0xffffffff
```

Injektovanje koda se pokreće ovako:

./eit386 -i object input_elf out_elf

object je naš objekat koji želimo da ubacimo u izvršni fajl

input_elf je izvršni fajl u koga ubacujemo objekat

out_elf je novi izvršni fajl sa ubačenim objektom

U direktorijumu programa nalaze se dva direktorijuma (**example.injection**, **example.protection**) u kojima se nalaze dvije skripte koje automatizuju proces injektovanja objekta i zaštite elf-a.

U direktorijumu **example.injection** takođe se nalazi **example.S** fajl koji je primjer asemblerskog koda za objekat koji injektujemo.

Realizacija i kompajliranje

Program je napisan u programskom jeziku C. Zasnovan je na algoritmu Silvia Cesara.

Za kompajliranje potreban je gcc kompajler i Makefile. Za korisnika dovoljno je da ukuca make naredbu i sudo make install naredbu za instaliranje programa.

Razvoj projekta možete pratiti na:

https://github.com/milan-stanojevic/eit386

Licenca