Verifikacija softvera - Vežbe

Ivan Ristović Ana Vulović

2022-10-10

Kolekcija materijala sa vežbi za kurs Verifikacija softvera na Matematičkom fakultetu, Univerziteta u Beogradu.

Teme i alati rađeni na vežbama:

- Debagovanje koristeći alate za debagovanje i razvojna okruženja
  - `gdb` - debagovanje koda na niskom nivou
  - `QtCreator` - debagovanje C/C++ kodova
  - `Intellij IDEA` - debagovanje Java koda
  - `Visual Studio` - debagovanje C, C++ i C# kodova
- Testiranje jedinica koda
  - Pisanje testabilnog koda
  - `QtTest` , `Catch` (C, C++)
  - `JUnit` (Java)
  - `xUnit` , `NUnit` (C#)
- Praćenje pokrivenosti koda testovima
  - `lcov` (C, C++)
  - `JaCoCo` (Java)
  - `dotnet-coverage` (C#)
- "Mock" testiranje
  - Pisanje *mock* klasa od nule (C++)
  - `Moq` (C#)
  - *Mock* testiranje baza podataka
- Profajliranje
  - `Valgrind` (memcheck, cachegrind, callgrind, hellgrind, drd)
  - `perf`
- Statička analiza
  - `KLEE`
  - `CBMC`
  - `Clang` statički analizator
- Alati i jezici za formalnu verifikaciju softvera
  - `Dafny`

Sadržaj

1 Debagovanje

1.1 QtCreator Debugger

QtCreator dolazi sa debugger-om koji predstavlja interfejs između QtCreator-a i native debugger-a (gdb, CDB, LLDB, ...). Moguće je debagovati Qt aplikacije, ali i native C/C++ aplikacije, kačiti se na već pokrenute procese i formirati debug sesije, i mnogo toga.

Više informacija je moguće pronaći u Qt dokumentaciji.

1.1.1 Buffer Overflow primer (QtCreator)

Ukoliko debagujemo Qt aplikacije, dovoljno je pokrenuti aplikaciju u Debug modu. Pokrenuti QtCreator i otvoriti BufferOverflow.pro projekat. Prilikom otvaranja projekta, QtCreator će otvoriti konfiguracioni dijalog - konfigurisati projekat sa podrazumevanim podešavanjima.

Napomena: QtCreator podrazumevano uključuje `clang` statički analizator ukoliko je on dostupan. Iako nije neophodno, ukoliko želite da sami pronađete probleme u izvornom kodu a tek potom proverite svoje pronalaske koristeći `clang` , isključite `clang` analizator u podešavanjima (`Edit -> Preferences -> Analyzer`).

Unutar QtCreator-a vidimo nekoliko pogleda (`Edit` , `Design` , `Debug` itd.). Trebalo bi da je `Edit` pogled već selektovan. Otvoriti `main.c` fajl i prodiskutovati o logici programa i njegovim slabim tačkama.

Unutar `Project` prozora možemo dodavati ili menjati postojeće konfiguracije za kompilaciju i pokretanje programa. To uključuje i dodavanje argumenata komandne linije (`Run` odeljak).

Pokrenuti debug sesiju. Isprobati debug akcije za kontrolisanje izvršavanja programa (`Debug` meni u glavnom meniju):

- `Interrupt`
- `Continue`
- `Step over`
- `Step into`
- `Step out`
- `Set/Remove breakpoint`

Možemo testirati ponašanje programa tako što prvo unesemo ispravnu lozinku `MyPassword` a zatim i proizvoljnu neispravnu lozinku (npr. `SomePassword`). Program se naizgled ispravno ponaša ali to ne znači da je u potpunosti ispravan.

Posmatrajući definicije promenljivih `password` i `ok`, možemo zaključiti da će se one na steku naći jedna do druge. Proverimo da li je zaista tako: desnim klikom na promenljive u prozoru za prikaz promenljivih na steku selektovati opciju `Open Memory Editor -> ... at object address ...`. Nastaviti izvršavanje i primetiti inicijalizaciju memorije za promenljivu `ok`. Pošto je promenljiva `password` neposredno pre promenljive `ok` u memoriji, i pošto se sadržaj promenljive `password` unosi sa standardnog ulaza, ukoliko uspemo da pređemo granice promenljive `password` onda možemo upisati proizvoljnu vrednost u promenljivu `ok` (pa i `"yes"`)!

Posmatrajmo isečak koda:

```
  scanf ("%s", password);
```

`scanf` nam ne garantuje da će učitati najviše `16` karaktera (koliko smo rezervisali za promenljivu `password`). Testirajmo ponašanje za niske dužine veće od 16 karaktera, npr. `WillThisPassNow?yes`. Vidimo da smo dobili privilegije iako lozinka nije ispravna.

Postavimo uslovni *breakpoint* nakon poziva `scanf`, da se program zaustavi ukoliko se promeni vrednost promenljive `ok`. Desnim klikom na `Breakpoint` i selekcijom opcije `Edit Breakpoint` možemo definisati uslov `ok != "no"` u `Condition` polju. Možemo takođe pratiti inicijalizaciju promenljive `ok` u `Memory Editor` -u. Nakon što se vrednost promeni, možemo je ručno vratiti na `"no"`.

Tok izvršavanja možemo pratiti i preko prikaza steka, odakle možemo videti redosled pozivanja funkcija. Konkretnu liniju u kodu koja je sledeća za izvršavanje, QT obeležava žutom strelicom levo od koda. Ukoliko se dogodi da smo mnogo napredovali i želimo da se pomerimo na neku ranije naredbu, dovoljno je da strelicu prevučemo na naredbu koja nam je potrebna, bez potrebe za ponovnim pokretanjem programa. Za ispekciju asemblerskog koda možemo otvoriti *Disassembler* prozor.

Ostaje pitanje - šta naš program radi ukoliko je lozinka toliko dugačka da prevazilazi veličinu steka (npr. `ThisPasswordSimplyExceedsMaximumLengthAvailableOnStack`)? Dobićemo poruku `*** stack smashing detected ***`. To je posledica opcije `gcc` -a `-fstack-protector` koja generiše zaštitnu promenljivu koja je se dodeljuje osetljivim funkcijama. Osetljivim se smatraju one funkcije koje koriste dinamičku alokaciju ili imaju bafere veće od `8B`. Zaštitna promenljiva se inicijalizuje pri ulasku u funkciju i proverava se na izlasku. Ukoliko provera ne bude tačna, štampa se prikazana poruka i program prekida sa izvršavanjem. Ukoliko želimo da učinom kod još ranjivijim na ovakve napade, možemo pomenutu zaštitu isključiti opcijom `-fno-stack-protector`. U slučaju Qt projekta potrebno je dodati ovu opciju u `QMAKE_CFLAGS` promenljivu. U definiciji projekta (datoteci ekstenzije `.pro`) uneti

sledeći red a zatim pozvati `qmake` i izvršiti ponovno prevoženje projekta:

```
QMAKE CFLAGS += -fno-stack-protector
```

Da bismo sprečili napade prekoračenjem bafera savet je da se primenjuju dobre programerske prakse i da se:

- preoverava upravljanje memorijom tokom programa koristeci neki od alata poput `valgrind memcheck`
- upotrebljava `fgets()` funkcije umesto `gets()` ili `scanf()` koje ne vrše provere granica promenljivih.
- upotrebljava `strncmp()` umesto `strcmp()` , `strncpy()` umesto `strcpy()` , itd.

1.1.1.1 Debagovanje spoljašnje aplikacije kroz QtCreator Ukoliko pokrenemo prethodni primer izvan QtCretor-a, to ne znači da ne možemo debagovati taj program. Štaviše, moguće je QtCreator debugger zakačiti za bilo koji program koji se izvršava ili će se tek izvršiti. Iz menija `Debug` biramo `Start Debugging` . Na raspolaganju su nam opcije:

- *Attach debugger to started application* - da bismo debagovali aplikaciju koja je već pokrenuta.
- *Attach debugger to unstarted application* - da bismo debagovali aplikaciju koja je će biti pokrenuta. Zadaje se putanja do izvršne verzije programa. Debugger će se aktivirati kada aplikacija bude pokrenuta.
- *Start and Debug External Application* - slično kao prethodno samo što će se program pokrenuti odmah. Možemo čekirati opciju da se doda tačka prekida na početak `main` funkcije.

Napomena: Ako QtCreator ne uspe da se poveže na proces, moguće je da treba da se dozvoli povezivanje na procese tako što se upiše `0` u fajl `/proc/sys/kernel/yama/ptrace_scope` .

Da bismo imali informacije o linijama izvornog koda koji odgovara programu koji se debaguje, potrebno je da taj program bude preveden sa uključenim debug informacijama (za `gcc` to je opcija `-g`). Inače, debugger će nam prikazivati memoriju kojoj pristupa program.

1.2 gdb

GNU Debugger (gdb) je debugger koji se može koristiti za debagovanje (najčešće) C/C++ programa. Preko gdb je moguće pokrenuti program sa proizvoljnim argumentima komandne linije, posmatrati stanje promenljivih ili registara procesora, pratiti izvršavanje kroz naredbe originalnog ili asembliranog koda, postavljanje bezuslovnih ili uslovnih tačaka prekida i sl. Više o gdb se može pročitati na ovom linku.

Koristeći gdb možemo učitati program iz prethodnog primera. U slučaju da želimo da ručno prevedemo program, neophodno je da se postaramo da je prosleđen `-g` flag `gcc` kompilatoru:

```
$ gcc main.c -g -o BufferOverflow
```

Pošto je QtCreator već preveo ovaj program i u `build-*` direktorijum ostavio izvršivi fajl, možemo ga direktno učitati u gdb:

```
$ gdb BufferOverflow
...
Reading symbols from BufferOverflow...
(gdb)
```

Alternativno, možemo program učitati u već pokrenuti gdb proces:

```
$ gdb
...
(gdb) file BufferOverflow
Reading symbols from BufferOverflow...
(gdb)
```

U slučaju da debug simboli nisu prisutni, možemo u definiciji projekta dodati odgovarajući flag (pod `QMAKE_CFLAGS`).

Spisak komandi koje gdb pruža možemo dobiti komandom `help` . Za sve ove naredbe postoje i skraćene varijante - npr. za `running` možemo kucati `run` ili samo `r` .

```
(gdb) help
List of classes of commands:

aliases -- User-defined aliases of other commands.
breakpoints -- Making program stop at certain points.
data -- Examining data.
files -- Specifying and examining files.
internals -- Maintenance commands.
obscure -- Obscure features.
running -- Running the program.
stack -- Examining the stack.
status -- Status inquiries.
support -- Support facilities.
text-user-interface -- TUI is the GDB text based interface.
tracepoints -- Tracing of program execution without stopping the program.
user-defined -- User-defined commands.
```

Tačke prekida možemo postaviti komandom `breakpoints` , aktiviramo/deaktiviramo

komandama `enable` / `disable` , a brišemo komandom `delete` . Komandom `continue` nastavljamo rad programa do naredne tačke prekida. Tačke prekida mogu biti linije, npr. `main.c:15` ali i funkcije, npr. `main` ili `main.c:grant_privilege` . Postavimo tačku prekida na funkciju `grant_privilege` , kontrolišimo izvršavanje programa naredbama `step` (nalik na *step into*) i `next` (nalik na *step over*):

```
(gdb) b main.c:grant_privilege
Breakpoint 1 at 0x1171: file ../01_buffer_overflow/main.c, line 5.
(gdb) r
Starting program: BufferOverflow
Breakpoint 1, grant_privilege () at ../01_buffer_overflow/main.c:5
5       {
(gdb) s
7               char ok[16] = "no";
(gdb) n
9               printf("\n Enter the password : \n");
(gdb) n

 Enter the password :
10              scanf("%s", password);
(gdb) n
MyPassword12        if (strcmp(password, "MyPassword")) {
(gdb) info locals
password = "MyPassword\000\367\377\177\000"
ok = "no", '\000' <repeats 13 times>
(gdb) n
15                      printf("\n Correct Password \n");
(gdb) n

 Correct Password
16                      strcpy(ok, "yes");
(gdb) n
19              if (strcmp(ok, "yes") == 0) {
(gdb) n
23                  printf("\n Root privileges given to the user \n\n");
(gdb) n

 Root privileges given to the user

25      }
(gdb) finish
Run till exit from
#0  grant_privilege () at ../01_buffer_overflow/main.c:25
```

```
main () at ../01_buffer_overflow/main.c:43
43              return 0;
```

Komandom `info` možemo dobiti informacije o lokalnim promenljivim, registrima itd. (npr. `info locals` tj. `info registers`). Komandom `info breakpoints` možemo videti spisak tačaka prekida.

Alternativno, moguće je iskoristiti drugačiji korisnički interfejs, komandom `tui` npr. `tui enable` . Tako dobijamo pogled na izvorni kod na jednoj polovini korisničkog interfejsa. Komandom `tui reg` možemo dobiti i prikaz registara sa `tui reg all` .

Koristeći gdb možemo dodati i uslovne tačke prekida, npr.:

```
(gdb) b grant_privilege:12 if ok != "no"
```

2 Pisanje testabilnog koda

Da bismo efikasno pisali testove jedinica koda, neophodno je da kod pišemo tako da bude pogodan za testiranje, ali i da softver razvijamo tako da je moguće paralelno pisati testove. Jedan način da se obezbedi takav način rada je razvoj vođen testovima (engl. *Test-Driven-Development*, skr. *TDD*). U situacijama kada već imamo dostupan izvorni kod i treba da napišemo testove jedinica koda, treba znati kako pristupiti pisanju testova i kako refaktorisati kod tako da bude pogodan za testiranje. Nekada funkcije koje treba da testiramo nemaju deterministički izlaz tako da ih je nemoguće testirati u izvornom obliku.

U ovom poglavlju će biti reči o tehnikama za pisanje testabilnog i skalabilnog koda. Primeri na kojima će ove tehnike biti prikazane su pisani u raznim programskim jezicima ali su koncepti koje prikazuju univerzalni, kao npr. inverzija zavisnosti, zamena implementacije itd.

2.1 C++ primer - kalkulator

Naš kod za kalkulator je nepodesan za jedinično testiranje jer se mnogo posla zapravo obavlja u main funkciji. Da bismo sve delove testirali moramo kod izdeliti na funkcije koje obavljaju po jednu celinu. Već postoje funkcije za svaku pojedinačnu operaciju koje imaju dva argumenta, njih nećemo dirati.

U `main` funkciji test podaci se učitavaju sa standardnog ulaza i sve se ispisuje na standardni izlaz. Da bismo mogli u jediničnim testovima da zadajemo svoje ulaze, promenićemo da funkcije ne učitavaju sa `std::cin` već sa proizvoljnog toka tipa `std::istream` , i da ispisuju ne na `std::cout` , već na proizvoljni tok tipa `std::ostream` . Na taj način ćemo izbeći učitavanje sa standardnog ulaza, a moći ćemo da unapred zadamo ulaz na kom se testira.

Iz tog razloga već postojećoj funkciji `showChoices` treba dodati argument `std::ostream & ostr` na koji će ispisivati ponudene opcije umesto na `std::cout` . Vidimo da se u `main` funkciji nakon prikaza opcije očekuje unos izbora operacije i proverava ispravosti unetog podatka. Taj deo objedinjen izdvajamo u posebnu funkciju `readChoice` koja će pozivati funkciju `showChoices` i učitavati opciju sa ulaznog toka sve dok se ne unese jedna od ispravnih cifara.

Nakon toga bi trebalo da se unesu dva operanda nad kojima će se primeniti izabrana operacija. To se može izdvojiti u posebnu funkciju `readOperands` koja će učitati dva realna broja sa ulaznog toka. Primenu odabrane operacije na unete operande na osnovu izabrane opcije izdvajamo u posebnu funkciju `calculate` . U njoj ćemo proveriti da li je opcija validna, primeniti operaciju i vratiti rezultat. Ukoliko se ne pošalje dobra vrednost argumenta `choice` funkcija bi, npr., mogla da baci izuzetak tipa `std::invalid_argument` ili vrati vrednost `false` . Proveru možemo uraditi i sa `assert(choice >= 1 && choice <= 4);` iz `cassert` zaglavlja. Ukoliko se ne

pošalje očekivana vrednost za argument `choice` program će biti prekinut. Ovo nam je način da nametnemo važenje preduslova za funkciju. Istu proveru bismo mogli da stavimo i u `printResults` funkciju. Dobili smo funkcije koje rade nezavisne poslove. Time su potencijalno upotrebljive i za neku dalju upotrebu ili pisanje kompleksnijeg kalkulatora. Sada i `main` funkcija može izgledati jednostavno kao niz poziva ovih funkcija.

2.2 Java OOP primer - Game of Life

Program predstavlja implementaciju poznate ćelijske automatizacije pod imenom Game of Life. Početna konfiguracija igre (početno stanje table kao i veličina mreže) su konfigurabilni. Stanje igre se ispisuje na standardni izlaz nakon svake iteracije.

Da bismo pisali testove jedinica koda, moramo razumeti odnose klasa u okviru aplikacije:

- paket `app` sadrži implementaciju `GameOfLife` igre
- paket `model` sadrži implementacije klasa `Cell` i `Grid` , koje se koriste za reprezentaciju stanja igre
  - paket `model.conf` sadrži implementacije početnih stanja igre (nasumičnu i jednu unapred kreiranu sa specifičnim osobinama, pod nazivom `Glider`)

Testovi koje bismo voleli da napišemo bi testirali:

- da li se mreža ispravno kreira na osnovu konfiguracije
- da li se pravila igre ispravno primenjuju iz generacije u generaciju
- da li se stanje igre ispravno ispisuje na standardni izlaz

Testove da li se mreža ispravno kreira na osnovu konfiguracije možemo lako napraviti. `Grid` klasa već implementira sve neophodno. Jedini problem predstavlja to što nemamo način da ručno postavimo konfiguraciju koja će se koristiti kao početna. Možemo testirati nasumičnu konfiguraciju međutim radije bismo da imamo determinističke testove. Takođe, naši testovi bi idealno testirali konfiguraciju u specijalnim slučajevima, npr. ivice mreže, što ne možemo kontrolisati nasumičnom konfiguracijom. Možemo ručno promeniti stanje klase `Grid` nakon kreiranja ali testovi **nikada** ne treba da zalaze u detalje implementacije klasa, tj. njihova stanja. Kreiranje ručnih determinističkih konfiguracija nam omogućava i testiranje pravila igre - možemo kreirati `Grid` objekat sa specifičnom konfiguracijom namenjenom da testira određeno pravilo igre ili kombinaciju više pravila, pozivajući metod `Grid.advance()` i testirati da li su se ćelije promenile onako kako bi trebalo. Zatim možemo testirati i specijalne slučajeve kao što su ivice mreže kao i situacije u kojima se na jednu ćeliju primenjuje više pravila.

Da bismo implementirali ručne konfiguracije, primetimo da je `model.conf.GliderConfiguration`

jedna implementacija ručne konfiguracije. Možemo da implementiramo naše specifične konfiguracije na sličan način, međutim imali bismo ponavljanje koda pošto bi se jedino menjao konstruktor klase. Apstrahujmo `GliderConfiguration` implementaciju - dodajemo klasu `ManualConfiguration` i menjamo klasu `GliderConfiguration` da nasleđuje klasu `ManualConfiguration` . Sada naše test konfiguracije mogu da instanciraju `ManualConfiguration` sa odgovarajućom konfiguracijom mreže, a takođe aplikacija može da se proširi dodavanjem novih predefinisanih konfiguracija.

Slično kao u kalkulator primeru, treba apstrahovati rad sa standardnim izlazom kako bismo mogli da testiramo prikaz stanja igre. Prikaz stanja se trenutno vrši u glavnoj klasi aplikacije, što takođe nije optimalno. Dodajmo `views` paket sa implementacijom `View` interfejsa koji predstavlja apstraktnu implementaciju prikaza aplikacije. Sada možemo kreirati implementaciju koja ispisuje stanje igre na proizvoljni izlazni tok (`PrintStreamView`) odnosno `System.out` ukoliko izlazni tok nije naveden. Logiku ispisa stanja igre pomeramo iz `app.GameOfLife` u `view.ConsoleView` .

2.3 C# - REST API klijent primer

Aplikacija je primer RESTful API klijenta koji prikazuje trenutnu temperaturu i dnevnu prognozu tako što kontaktira servis OpenWeather, tačnije njegov API server (*Napomena: pokretanje primera zahteva ključ koji aplikacija traži u fajlu* ***`key.txt`***). Detalji funkcionalnosti ovog servisa nisu od značaja za razumevanje ovog primera. Pojednostavljeno, klijent će serveru poslati HTTP zahtev za odgovarajućim resursom (trenutna temperatura, prognoza, i sl.) i server će poslati objekat sa odgovarajućim informacijama serijalizovanim u JSON. Pogledajmo implementaciju:

- prostor imena `Common` sadrži klase koje se koriste za deserijalizaciju odgovora servera
- prostor imena `Services` sadrži klasu `WeatherService` koja će biti meta naših testova
- glavni prostor imena koristi `WeatherService` da prikaže trenutnu temperaturu i prognozu za odgovarajući upit

Da bismo pisali testove za klasu `WeatherService` , pogledajmo njen javni interfejs (to što su neke funkcije asinhrone nema uticaj na suštinu primera):

```
bool IsDisabled();
async Task<CompleteWeatherData?> GetCurrentDataAsync(string query);
async Task<Forecast?> GetForecastAsync(string query);
```

Metod `IsDisabled` može lako da se testira kreiranjem servisa bez ključa. Druge metode, međutim, nisu toliko jednostavne pošto u sebi rade više od jednog posla - kreiranje HTTP zahteva, slanje zahteva, primanje odgovora i deserijalizacija odgovora. Ukoliko bismo testirali ove metode bez ikakve izmene, onda bismo stalno slali HTTP

zahteve servisu u našim testovima - što je sporo i nepovoljno. Štaviše, nemoguće je ovako testirati ponašanje naše implementacije u slučaju da server vrati nevalidan ili nekompletan odgovor. Čak i da možemo nekako rešiti sve te problema, ne možemo znati unapred koje odgovore servera da očekujemo - temperaturu i prognozu ne možemo znati unapred. Možemo pokrenuti lokalnu instancu OpenWeather servera modifikovanu za naše potrebe ali to nije optimalno rešenje. Oba ova problema (nedeterminističnost rada servisa i testiranje višestrukih funkcionalnosti jednog metoda) možemo rešiti tako što ručno ubrizgamo odgovor servera. Trenutna implementacija nam to ne dozvoljava, tako da hajde da je modifikujemo, ali ujedno i proširimo.

Pre svega, preimenujmo `WeatherService` u `OpenWeatherService` i apstrahujmo interfejs ove klase `IWeatherService`. Kontaktiranje servera možemo apstrahovati u logiku klase `WeatherHttpService`. U našim testovima, možemo koristiti implementaciju nalik na onu u klasi `TestWeatherHttpService`. Ne želimo da `OpenWeatherService` direktno koristi `WeatherHttpService` pošto nam to ne omogućava zamenu implementacije klase `WeatherHttpService` klasom `TestWeatherHttpService` u našim testovima. Stoga kreirajmo interfejs `IWeatherHttpService` koji će implementirati klase `WeatherHttpService` i `TestWeatherHttpService`. Sada klasa `OpenWeatherService` može da ima zavisnost na interfejs u konstruktoru (što dodatno omogućava druge povoljnosti kao što je ubrizgavanje zavisnosti).

3 Instalacije

3.1 Alati za debagovanje i razvojna okruženja

3.1.1 QtCreator

Instalirati QtCreator sa zvanične stranice. Alternativno, moguće je i instalirati ceo Qt radni okvir koji uključuje i QtCreator.

Za neke Linux distribucije je dostupan paket `qt<VERZIJA>-creator` .

3.1.2 gdb

Za većinu Linux distribucija je dostupan paket `gdb` . `gdb` je za neke distribucije deo paketa za razvoj (npr. `build-essential` za Ubuntu).