

Wednesday, June 26, 2024 at 04:16:01 Central European Summer Time

---

**Subject:** [DIPLOMSKI IZVJEŠĆE] Lovro Grgurić Mileusnić  
**Date:** Sunday, 9 June 2024 at 17:22:12 Central European Summer Time  
**From:** Lovro Grgurić-Mileusnić  
**To:** Stjepan Groš  
**Attachments:** diplomski\_demo-2024-06-03\_18.44.35.mp4, lovro\_grguricmileusnic\_31\_05\_2024.pdf

Poštovani profesore,

Šaljem Vam izvješće za posljednja dva tjedna.

U tjednu do 31.5. sam krenuo raditi CAN zadatak kao zadatak kao primjer zadatka s više ECU-ova te napravljenu TUI ploču s instrumentima. Jedan ECU šalje podatke o stanju automobila (brzina, pokazivači smjera, stanje motora, pojaseva, vrata), a drugi ih prima i prikazuje na ploči. Ideja zadatka je da natjecatelj pokrene slanje primjera CAN okvira te da uspije snimanjem prometa i korištenjem alata poput [cansniffera](#) reverzati pakete i pogurati brzinu preko 230km/h te upaliti pokazivače smjera. Nakon toga se zastavica prikazuje na TUI ploči s instrumentima.

U prethodnom tjednu sam dovršio navedeni zadatak i krenuo pisati diplomski rad. U prilogu je video koji demonstrira zadatak, ali sa ugašenim generiranjem nasumičnih paketa na sabirnici, kako bi se bolje vidjelo što se zapravo događa.

Lijep pozdrav,  
Lovro Grgurić Mileusnić

Wednesday, June 26, 2024 at 04:16:01 Central European Summer Time

---

**Subject:** [DIPLOMSKI IZVJEŠĆE] Lovro Grgurić Mileusnić  
**Date:** Wednesday, 29 May 2024 at 15:19:21 Central European Summer Time  
**From:** Lovro Grgurić-Mileusnić  
**To:** Stjepan Groš  
**Attachments:** lovro\_grguricmileusnic\_24\_05\_2024.pdf, WhatsApp Image 2024-05-28 at 00.22.22.jpeg

Poštovani profesore,

Šaljem Vam izvješće za prethodni tjedan. Pokušao sam pokrenuti i kontejnerizirati AGL ploču s instrumentima, ali sam naišao na niz problema zbog kojih sam od toga odustao. Prvotno sam imao problema s lokalnim pokretanjem kompajliranjem i pokretanjem pa s kontejneriziranjem. Naposljetku sam uspio pokrenuti aplikaciju u kontejneru s X11 forwardingom jer moja Linux distribucija ne podržava Flutter, ali sam stao na novom problemu s Flutter rendererom, kojem nisam uspio naći rješenje.

Odustao sam od navedene aplikacije i napravio [svoj jednostavni TUI](#), koji se učitava povezivanjem na kontejner korištenjem SSH. Koristio sam golang biblioteke Bubbletea i Wish za stvaranje SSH TUI aplikacija. Ovime se i olakšava udaljeno spajanje na CTF.

Prikaz je moguće ažurirati kroz HTTP zahtjeve koje šalje kontejner s ECU kodom:



Trenutno izrađujem CAN zadatak koji koristi ovaj TUI.

Lijep pozdrav,  
Lovro Grgurić Mileusnić

**Wednesday, June 26, 2024 at 04:16:01 Central European Summer Time**

---

**Subject:** [DIPLOMSKI IZVJEŠĆE] Lovro Grgurić Mileusnić  
**Date:** Wednesday, 22 May 2024 at 00:46:33 Central European Summer Time  
**From:** Lovro Grgurić-Mileusnić  
**To:** Stjepan Groš  
**Attachments:** lovro\_grguricmileusnic\_17\_05\_2024.pdf

Poštovani profesore,

Drugu polovicu prošlog tjedna proveo sam na STEM Gamesu te nisam mogao raditi na diplomskom radu. Pokušao sam to nadoknaditi u prethodna 4 dana.

U prethodnom izvješću sam naveo da se zbog kompleksnosti konfiguriranja sučelja iz Automotive Grade Linux projekta, možda više isplati napraviti tekstualno sučelje kojem bi se pristupalo kroz naredbeni redak. Svedjedno sam pokušao prvo pokrenuti ga lokalno, ali sam naišao na niz problema s inačicama Java, Fluttera i Darta. Osim za Dart, autor nije specificirao koje je inačice Java i Flutter SDK-ova potrebno koristiti, ali sam uspio doći do prikladnih inačica iz grešaka prilikom pokretanja. Naknadno sam shvatio da je za Flutter desktop aplikacije potrebna Ubuntu ili Debian distribucija koju ne koristim. Preostalo mi je pokušati kontejnerizirati aplikaciju skupa s pripadajućim KUKSA serverom s Ubuntu imageom kao bazom.

Uz to dodao sam mogućnost dodavanja "listenera" na stanje ECU-a, kako bih mogao prosljeđivati promjene stanja i prikazivati ih na GUI-ju.

Istražio sam dostupne TUI biblioteke s namjerom da napravim vlastito jednostavno

sučelje. Skicirao sam moguće "arhitekture" za korištenje web GUI-ja ili TUI-ja te sučelja iz AGL projekta.

U ostatku tjedna, pokušat ću kontejnerizirati sučelje iz AGL projekta ili napraviti svoje, kako bih mogao napraviti zadatak s "običnim" CAN-om.

Lijep pozdrav,  
Lovro Grgurić Mileusnić

**Wednesday, June 26, 2024 at 04:16:01 Central European Summer Time**

---

**Subject:** [DIPLOMSKI IZVJEŠĆE] Lovro Grgurić Mileusnić  
**Date:** Monday, 13 May 2024 at 18:06:05 Central European Summer Time  
**From:** Lovro Grgurić-Mileusnić  
**To:** Stjepan Groš  
**Attachments:** lovro\_grguricmileusnic\_03\_05\_2024.pdf, lovro\_grguricmileusnic\_10\_05\_2024.pdf

Poštovani profesore,

Ispričavam se zbog kasnog slanja izvješća, ovo su izvješća za 3. i 10. svibnja.

Tijekom prethodnog tjedna dovršio sam drugi UDS zadatak koji simulira ranjivi 0x27 Security Access UDS servis te sam osmislio još nekoliko zadataka koji kombiniraju korištenje UDS i CAN protokola. Imao sam namjeru napraviti zadatak s XCP protokolom te sam pročitao nekoliko dokumenata i članaka koji ga opisuju. Imao sam namjeru napraviti sličan zadatak kao s UDS-om, gdje korisnik mora iskoristiti loše konfigurirani XCP UNLOCK, koji je ekvivalent UDS-ovom Security Access servisu.

Tijekom prethodnog tjedna sam dodao XCP u program predložak ECU-a, koristeći Scapy. Tijekom pisanja koda za zadatak sam shvatio da Scapy nema način za razlikovati XCP zahtjeve i odgovore te sve pakete automatski parsira kao odgovore (jer je biblioteka namijenjena za komunikaciju s pravim ECU-om). Privremeno sam odustao od izrade navedenog zadatka te sam se usmjerio na omogućavanje povezivanje ECU-a s nekom vrstom GUI-ja. Ploča s instrumentima iz Automotive Grade Linux projekta mi se činila korisna za ovu potrebu, ali zahtjeva postavljanje testnih TLS certifikata, generiranje JSON Web Tokena, OpenStreetMap API ključa. Uz to, ako želim da se sve pokreće korištenjem Docker Composea, korisnik bi se trebao spojiti na aplikaciju s pomoću VNC-a ili X11 forwardinga. Za pokazni primjer, mislim da je brže i jednostavnije napraviti jednostavan prikaz brzine, pokazivača smjera i sličnog korištenjem neke Terminal UI biblioteke. Takvo sučelje može se prikazivati bez dodatne konfiguracije, korištenjem `--tty` i `--interactive` opcija pri pokretanju kontejnera. Dodatno se može prilagoditi za prikaz zastavice nakon što su postignuti određeni uvjeti.

U ovom tjednu namjeravam izraditi navedeno sučelje te zadatak koji ga koristi.

Lijep pozdrav,  
Lovro Grgurić Mileusnić

**Wednesday, June 26, 2024 at 04:16:01 Central European Summer Time**

---

**Subject:** RE: [DIPLOMSKI] Zadatak za Hackultet  
**Date:** Friday, 3 May 2024 at 13:40:07 Central European Summer Time  
**From:** Benjamin Nadarević  
**To:** Lovro Grgurić-Mileusnić, Stjepan Groš, Predrag Pale  
**CC:** Marin Vuković, Ante Đerek

Pozdrav,

Finale je planirano za kraj 8. illi početak 9. mjeseca.

S poštovanjem,  
Benjamin Nadarević

---

From: Lovro Grgurić-Mileusnić [[Lovro.Grguric-Mileusnic@fer.hr](mailto:Lovro.Grguric-Mileusnic@fer.hr)]  
Sent: Thursday, May 02, 2024 7:59 PM  
To: Benjamin Nadarević; Stjepan Groš; Predrag Pale  
Cc: Marin Vuković; Ante Đerek  
Subject: Odg: [DIPLOMSKI] Zadatak za Hackultet

Poštovani,

Što se tiče otežavanja varanja, uklonio sam ljske iz /bin direktorija kontejnera, ali kao što ste spomenuli, natjecatelj to lagano može zaobići ako ima root ovlasti u virtualki.

Uz opciju za udaljen pristup koju ste opisali, razmatrao sam i korištenje canelloni <https://github.com/mguentner/cannelloni> "CANoverTCP" tunela. Natjecatelji onda mogu koristiti alate i skripte za rješavanje zadatka na vlastitom računalu. Svakom natjecatelju ili timu može biti dodijeljen TCP port na udaljenom računalu s postavljenim kontejnerima. Sve skupa se onda može brzo postaviti kroz Docker compose konfiguraciju s onoliko kontejnera koliko ima natjecatelja/timova.

Iako većina modernih verzija popularnih Linux distribucija sadrže potrebne module jezgre, potencijalno se natjecateljima može podijeliti slika virtualne mašine koja ih već ima učitane. Uz to, na istu virtualnu mašinu može se odmah instalirati i can-utils paket kao i alati Scapy i caringcaribou koji su potrebni za rješavanje zadatka.

Trenutno u sklopu diplomskog rada izrađujem kompleksniju varijantu ovog zadatka (protokol UDS) te imam u planu izraditi zadatak s protokolom XCP te običnim CAN-om.

Slažem se da bi bilo bolje da je zadatak dio finala bootcampa te po potrebi mogu modificirati format zastavice prema formatu koji će se koristiti na CTF-u.

Otprilike kojeg datuma je planirano finale?

Lijep pozdrav,  
Lovro Grgurić Mileusnić

Šalje: Benjamin Nadarević <[benjamin.nadarevic@lss.hr](mailto:benjamin.nadarevic@lss.hr)>

Poslano: 2. svibnja 2024. 19:14

Prima: Stjepan Groš <[Stjepan.Gros@fer.hr](mailto:Stjepan.Gros@fer.hr)>; Predrag Pale <[Predrag.Pale@lss.hr](mailto:Predrag.Pale@lss.hr)>

Kopija: Marin Vuković <[Marin.Vukovic@fer.hr](mailto:Marin.Vukovic@fer.hr)>; Ante Đerek <[Ante.Derek@fer.hr](mailto:Ante.Derek@fer.hr)>; Lovro Grgurić-Mileusnić <[Lovro.Grguric-Mileusnic@fer.hr](mailto:Lovro.Grguric-Mileusnic@fer.hr)>

Predmet: RE: [DIPLOMSKI] Zadatak za Hackultet

Pozdrav,

Nismo ga stigli detaljno proučiti ali po kratkom pregledu nam izgleda jako zanimljivo. Nismo sigurni koji bi bio najbolji način da ga distribuiramo natjecateljima, a da ne mogu lagano varati.

Ako dobro shvaćam, natjecatelj mora moći pokretati kod na istom hostu na kojem je docker kontejner kako bi mogao imati interakciju s njim i izvući memoriju binarya.

Ako im to distribuiramo u formi Linux virtualke u kojoj se pokreće docker kontejner, natjecatelji mogu trivijalno dobiti root pristup toj virtualki a nakon toga i shell na docker kontejneru i tako zaobilazno doći do flaga. Naravno, nije problem ako natjecatelj smisli svoj način da dođe do flaga, ali problem je ako je taj način puno lakši od namijenjenog.

Čini nam se da bi bilo najbolje kada bi natjecatelji imali remote non-root pristup nekom serveru gdje se ovaj docker kontejner pokreće, pa da moraju riješiti zadatak na više-manje namijenjen način, ali takvo nešto nije bilo predviđeno kad smo postavljali infrastrukturu za ovu instancu Hackulteta.

Zato predlažem da ovaj (a i druge zadatke iz područja sigurnosti automobila, ako su planirani) iskoristimo u finalu bootcampa kada budemo odlučivali tko od natjecatelja ulazi u ECSC tim.

S poštovanjem,  
Benjamin Nadarević

---

From: Stjepan Groš [[Stjepan.Gros@fer.hr](mailto:Stjepan.Gros@fer.hr)]

Sent: Thursday, May 02, 2024 6:32 PM

To: Predrag Pale; Benjamin Nadarević

Cc: Marin Vuković; Ante Đerek; Lovro Grgurić-Mileusnić

Subject: RE: [DIPLOMSKI] Zadatak za Hackultet

Pozdrav!

Možete li mi dati kakvu povratnu informaciju u vezi ovoga?

Stavio sam studenta u CC ako treba reagirati da bude brže.

SG

From: Stjepan Groš

Sent: Thursday, April 25, 2024 10:35 AM

To: Predrag Pale <[Predrag.Pale@lss.hr](mailto:Predrag.Pale@lss.hr)>; benjamin.nadarevic <[benjamin.nadarevic@lss.hr](mailto:benjamin.nadarevic@lss.hr)>

Cc: Marin Vuković <[Marin.Vukovic@fer.hr](mailto:Marin.Vukovic@fer.hr)>; Ante Đerek <[Ante.Derek@fer.hr](mailto:Ante.Derek@fer.hr)>

Subject: Fwd: [DIPLOMSKI] Zadatak za Hackultet

Pozdrav!

Diplomand koji radi sustav za generiranje zadataka iz autoindustrije, napravio je jedan CTF zadatak pa ga prosljeđujem.

SG

----- Forwarded Message -----

Subject:

[DIPLOMSKI] Zadatak za Hackultet

Date:

Thu, 25 Apr 2024 02:11:21 +0200

From:

Lovro Grgurić-Mileusnić <[Lovro.Grguric-Mileusnic@fer.hr](mailto:Lovro.Grguric-Mileusnic@fer.hr)><mailto:[Lovro.Grguric-Mileusnic@fer.hr](mailto:Lovro.Grguric-Mileusnic@fer.hr)>

To:

Stjepan Groš <[Stjepan.Gros@fer.hr](mailto:Stjepan.Gros@fer.hr)><mailto:[Stjepan.Gros@fer.hr](mailto:Stjepan.Gros@fer.hr)>

Poštovani profesore,

Šaljem Vam zip arhivu s tekstom zadatka, uputama za postavljanje te opisom predviđenog rješenja skupa s pripadajućom Python skriptom.

Lijep pozdrav,  
Lovro Grgurić Mileusnić

---

**Wednesday, June 26, 2024 at 04:16:01 Central European Summer Time**

---

**Subject:** [DIPLOMSKI IZVJEŠĆE] Lovro Grgurić Mileusnić  
**Date:** Saturday, 27 April 2024 at 13:18:26 Central European Summer Time  
**From:** Lovro Grgurić-Mileusnić  
**To:** Stjepan Groš

Poštovani profesore,

Ovaj tjedan dovršio sam prvi CTF zadatak koji sam Vam već dostavio u zasebnom mailu. Kako bi se Docker container koji sadrži zadatak uspješno pokrenuo potrebno ga je prvo dodati u mrežu stvorenu s dockercan Docker network driver pluginom. Zadatak i plugin su postavljeni na Dockerhub. Trenutno dovršavam drugi zadatak u kojem je cilj iskoristiti UDS kao i u prvom. Popravio sam grešku u pluginu koju sam spomenuo na sastanku,

tako da bi sada trebao normalno raditi kod uklanjanja i ponovnog dodavanja containera u mrežu.

Daljnji plan mi je izraditi još CTF zadataka, ovo je trenutni popis:

- Čitanje iz memorije pomoću XCP-a
- Zadaci s GUI-jem ploče s instrumentima
  - Iskorištavanje UDS Routine Control servisa
  - Snimanje CAN prometa, reverziranje poruka i replay napadi (otključavanje vrata, žmigavci, brzina, broj okretaja, odometar)
- MITM napad na UDS SecurityAccess ili Authentication preko dvije sabirnice
- UDS WriteDataByIdentifier ili WriteMemoryByAddress zadatak

Paralelno uz izradu zadataka ću dorađivati ECU predložak.

Lijep pozdrav,  
Lovro Grgurić Mileusnić

---

**Wednesday, June 26, 2024 at 04:16:01 Central European Summer Time**

---

**Subject:** RE: [DIPLOMSKI] Zadatak za Hackultet i pitanja  
**Date:** Thursday, 2 May 2024 at 18:31:19 Central European Summer Time  
**From:** Stjepan Groš  
**To:** Lovro Grgurić-Mileusnić

Nisam dobio nikakav povrati odgovor. Pitat ću ih...

SG

---

**From:** Lovro Grgurić-Mileusnić <[Lovro.Grguric-Mileusnic@fer.hr](mailto:Lovro.Grguric-Mileusnic@fer.hr)>  
**Sent:** Thursday, May 2, 2024 4:50 PM  
**To:** Stjepan Groš <[Stjepan.Gros@fer.hr](mailto:Stjepan.Gros@fer.hr)>  
**Subject:** Re: [DIPLOMSKI] Zadatak za Hackultet i pitanja

Poštovani profesore,

Htio sam provjeriti samo je li potrebno da još nešto poduzmem ili pomognem vezano uz postavljanje zadatka na CTF. Jeste li dobili odgovor od organizatora?

Lijep pozdrav,  
Lovro Grgurić Mileusnić

---

On Apr 25, 2024 at 2:11 AM, <[Lovro.Grguric-Mileusnic@fer.hr](mailto:Lovro.Grguric-Mileusnic@fer.hr)> wrote:

Poštovani profesore,

Šaljem Vam zip arhivu s tekstom zadatka, uputama za postavljanje te opisom predviđenog rješenja

skupa s pripadajućom Python skriptom.

Lijep pozdrav,  
Lovro Grgurić Mileusnić

---

**Šalje:** Stjepan Groš <[Stjepan.Gros@fer.hr](mailto:Stjepan.Gros@fer.hr)>

**Poslano:** 16. travnja 2024. 23:46

**Prima:** Lovro Grgurić-Mileusnić <[Lovro.Grguric-Mileusnic@fer.hr](mailto:Lovro.Grguric-Mileusnic@fer.hr)>

**Predmet:** Re: Odg: [DIPLOMSKI IZVJEŠĆE] Lovro Grgurić Mileusnić

On 16. 04. 2024. 12:12, Lovro Grgurić-Mileusnić wrote:

Poštovani profesore,

Je li "Hackultet" CTF za koji ste spomenuli da bi možda mogli plasirati zadatak vezan za automobile? Vidio sam da su otvorene [prijave](#) te da kreće 3. svibnja.

Ako je to još uvijek mogućnost, mislim da mogu osmisлити i napraviti jednostavan zadatak do polovice idućeg tjedna.

Da, to je to. AJd' napravite zadatak pa cu vidjeti da se uvrsti u listu zadataka.

SG

Lijep pozdrav,  
Lovro Grgurić Mileusnić

---

**Šalje:** Lovro Grgurić-Mileusnić

**Poslano:** 16. travnja 2024. 12:02

**Prima:** Stjepan Groš <[Stjepan.Gros@fer.hr](mailto:Stjepan.Gros@fer.hr)>

**Predmet:** [DIPLOMSKI IZVJEŠĆE] Lovro Grgurić Mileusnić

Poštovani profesore,

U prethodnom tjednu sam programirao temelj (predložak) za sve ECU-ove, u koji se onda može dodati konkretna implementacija željene logike. Predložak podržava CAN 2.0 i CAN FD poruke na sloju podatkovne poveznice te ISO-TP na u transportnom sloju. Obzirom da ISO-TP sam po sebi nije vrlo zanimljiv u pogledu CTF zadataka, neću ga posebno isticati kao nešto što treba konfigurirati, nego ću povrh njega napraviti predložak za UDS.

Za ISO-TP sam pronašao python biblioteku can-isotp, koja može za CAN sloj koristiti python-can, što mi se tada činilo prikladnim s obzirom na to da ga koristim za CAN i CAN FD poruke. Python-can već pruža "Notifier" objekte koji iz zasebne daemon dretve obavještavaju glavni program o pristiglim porukama na CAN\_RAW socket. "Notifier" objekte koristi i can-isotp biblioteka, ali ne pruža obavještavanje već ih koristi interno za komunikaciju s CAN slojem, a korisniku biblioteke daje samo recv() i send() metode na korištenje. Pokušao sam napraviti svoj ISO-TP "Notifier" povrh tih metoda, ali nije dosljedno funkcionirao te je sama implementacija ISO-TP protokola u can-isotp



biblioteci bila nekompatibilna s postojećim ISO-TP socketcan alatima (isotpsend, isotprecv...). Rješenje je bilo koristiti ISO-TP sockete direktno u vlastitom "Notifier" objektu, umjesto python-can i can-isotp biblioteka.

Preostalo mi je još dodati mogućnost konfiguriranja periodičkog slanja poruka za što ću koristiti CAN\_BCM iz socketcana te dodati dio predloška za implementaciju komunikacije ECU programa s GUI-jem. Mislim da ću ovaj tjedan stići napraviti prvi CTF zadatak. Za kraj ću ostaviti skriptu za generiranje compose.yml-a i pripadajućeg projekta s ECU predlošcima iz kojeg je moguće implementirati vlastiti CTF zadatak ili simulaciju.

Lijep pozdrav,  
Lovro Grgurić Mileusnić

--

associate professor Stjepan Groš, Ph.D.

[Laboratory for Information Security and Privacy](#)

[Faculty of Electrical Engineering and Computing](#)

[University of Zagreb](#)

Tel: +385 (0)1 6129 943

Mob: +385 (0)91 6454 982

Fax: +385 (0)1 6129 653

E-mail: [stjepan.gros@fer.hr](mailto:stjepan.gros@fer.hr)

Web: <https://www.fer.unizg.hr/stjepan.gros>

**Wednesday, June 26, 2024 at 04:16:01 Central European Summer Time**

---

**Subject:** [DIPLOMSKI IZVJEŠĆE] Lovro Grgurić Mileusnić  
**Date:** Thursday, 25 April 2024 at 02:01:50 Central European Summer Time  
**From:** Lovro Grgurić-Mileusnić  
**To:** Stjepan Groš  
**Attachments:** lovro\_grguricmileusnic\_19\_04\_2024.pdf

Poštovani profesore,

U prethodnom tjednu (do 19.4.) odustao sam od biblioteka python-can i python-can-isotp u korist Scapyu, koji podržava oba navedena protokola kroz socketcan sockete, ali i protokole UDS, OBD i XCP u aplikacijskom sloju. Time sam izgubio dio apstrakcija koje su te biblioteke nudile pa sam dio tjedna potrošio na prebacivanju na Scapy. Dovršio sam osnovni predložak za ECU programe (CAN i UDS) te osmislio dva zadatka temeljena na iskorištavanju loše implementiranih UDS servisa.

Tijekom ovog tjedna proučavao sam na koji način radi alat caringcaribou kako bih znao što sve minimalno trebam implementirati u programu simuliranog ECU-a, a da se alat ponaša kao u interakciji sa stvarnim ECU-om. Dovršio sam implementaciju jednostavnijeg od ta dva zadatka, što je uključivalo doradivanje mog network driver plugina te njegovo pakiranje i postavljanje na dockerhub. U petak ću Vam poslati potpuno izvješće i bilješke za trenutni tjedan.

Lijep pozdrav,  
Lovro Grgurić Mileusnić

**Wednesday, June 26, 2024 at 04:16:01 Central European Summer Time**

---

**Subject:** Re: Odg: Odg: [DIPLOMSKI IZVJEŠĆE] Lovro Grgurić Mileusnić  
**Date:** Wednesday, 24 April 2024 at 15:58:13 Central European Summer Time  
**From:** Stjepan Groš  
**To:** Lovro Grgurić-Mileusnić

Dođite onda do mene u petak u 14 sati.

SG

On 24. 04. 2024. 13:51, Lovro Grgurić-Mileusnić wrote:

Poštovani profesore,

Odgovara mi bilo koji termin sutra i preksutra za sastanak.

Dovršio sam jednostavniju varijantu zadatka za CTF te trenutno radim na pakiranju i postavljanju containera i plugina na dockerhub, kako bi ga natjecatelji ili organizatori mogli pokrenuti kroz nekoliko docker naredbi. Ako će jednostavnija varijanta zadatka biti prikladna organizatorima, krenuo sam raditi i težu varijantu za veći broj bodova.

Ispričavam se zbog premašivanja rokova za izvješća, nekad mi ih je lakše sastaviti kad zaokružim ono što sam naumio za određeni period. Ubuduće ću se pridržavati rokova.

Danas ću Vam poslati izvješće i bilješke za prethodni tjedan.

Lijep pozdrav,  
Lovro Grgurić Mileusnić

---

**Šalje:** Stjepan Groš <[Stjepan.Gros@fer.hr](mailto:Stjepan.Gros@fer.hr)>  
**Poslano:** 23. travnja 2024. 15:51  
**Prima:** Lovro Grgurić-Mileusnić <[Lovro.Grguric-Mileusnic@fer.hr](mailto:Lovro.Grguric-Mileusnic@fer.hr)>  
**Predmet:** Re: Odg: [DIPLOMSKI IZVJEŠĆE] Lovro Grgurić Mileusnić

Kolega,

što kažete da se ovaj nađemo i porazgovaramo što je napravljeno?

Također, zamolio bi vas da se pridržavate rokova za slanje izvješća.

SG

On 16. 04. 2024. 12:12, Lovro Grgurić-Mileusnić wrote:

Poštovani profesore,

Je li "Hackultet" CTF za koji ste spomenuli da bi možda mogli plasirati zadatak vezan za automobile? Vidio sam da su otvorene [prijave](#) te da kreće 3. svibnja.

Ako je to još uvijek mogućnost, mislim da mogu osmisliti i napraviti jednostavan zadatak do polovice idućeg tjedna.

Lijep pozdrav,  
Lovro Grgurić Mileusnić

---

**Šalje:** Lovro Grgurić-Mileusnić

**Poslano:** 16. travnja 2024. 12:02

**Prima:** Stjepan Groš <[Stjepan.Gros@fer.hr](mailto:Stjepan.Gros@fer.hr)>

**Predmet:** [DIPLOMSKI IZVJEŠĆE] Lovro Grgurić Mileusnić

Poštovani profesore,

U prethodnom tjednu sam programirao temelj (predložak) za sve ECU-ove, u koji se onda može dodati konkretna implementacija željene logike. Predložak podržava CAN 2.0 i CAN FD poruke na sloju podatkovne poveznice te ISO-TP na u transportnom sloju. Obzirom da ISO-TP sam po sebi nije vrlo zanimljiv u pogledu CTF zadataka, neću ga posebno isticati kao nešto što treba konfigurirati, nego ću povrh njega napraviti predložak za UDS.

Za ISO-TP sam pronašao python biblioteku can-isotp, koja može za CAN sloj koristiti python-can, što mi se tada činilo prikladnim s obzirom na to da ga koristim za CAN i CAN FD poruke. Python-can već pruža "Notifier" objekte koji iz zasebne daemon dretve obavještavaju glavni program o pristiglim porukama na CAN\_RAW socket. "Notifier" objekte koristi i can-isotp biblioteka, ali ne pruža obavještavanje već ih koristi interno za komunikaciju s CAN slojem, a korisniku biblioteke daje samo recv() i send() metode na korištenje. Pokušao sam napraviti svoj ISO-TP "Notifier" povrh tih metoda, ali nije dosljedno funkcionirao te je sama implementacija ISO-TP protokola u can-isotp biblioteci bila nekompatibilna s postojećim ISO-TP socketcan alatima (isotpsend, isotprecv...). Rješenje je bilo koristiti ISO-TP sockete direktno u vlastitom "Notifier" objektu, umjesto python-can i can-isotp biblioteka.

Preostalo mi je još dodati mogućnost konfiguriranja periodičkog slanja poruka za što ću koristiti CAN\_BCM iz socketcana te dodati dio predložka za implementaciju komunikacije ECU

programa s GUI-jem. Mislim da ću ovaj tjedan stići napraviti prvi CTF zadatak. Za kraj ću ostaviti skriptu za generiranje compose.yml-a i pripadajućeg projekta s ECU predloščima iz kojeg je moguće implementirati vlastiti CTF zadatak ili simulaciju.

Lijep pozdrav,  
Lovro Grgurić Mileusnić

--

associate professor Stjepan Groš, Ph.D.  
[Laboratory for Information Security and Privacy](#)  
[Faculty of Electrical Engineering and Computing](#)  
[University of Zagreb](#)  
Tel: +385 (0)1 6129 943  
Mob: +385 (0)91 6454 982  
Fax: +385 (0)1 6129 653  
E-mail: [stjepan.gros@fer.hr](mailto:stjepan.gros@fer.hr)  
Web: <https://www.fer.unizg.hr/stjepan.gros>

--

associate professor Stjepan Groš, Ph.D.  
[Laboratory for Information Security and Privacy](#)  
[Faculty of Electrical Engineering and Computing](#)  
[University of Zagreb](#)  
Tel: +385 (0)1 6129 943  
Mob: +385 (0)91 6454 982  
Fax: +385 (0)1 6129 653  
E-mail: [stjepan.gros@fer.hr](mailto:stjepan.gros@fer.hr)  
Web: <https://www.fer.unizg.hr/stjepan.gros>

**Wednesday, June 26, 2024 at 04:16:01 Central European Summer Time**

---

**Subject:** [DIPLOMSKI IZVJEŠĆE] Lovro Grgurić Mileusnić  
**Date:** Wednesday, 10 April 2024 at 00:12:35 Central European Summer Time  
**From:** Lovro Grgurić-Mileusnić  
**To:** Stjepan Groš  
**Attachments:** lovro\_grguricmileusnic\_05\_04\_2024.pdf

Poštovani profesore,

U prethodnom tjednu sam htio započeti pisanje koda za simulirane ECU-ove, međutim naišao sam na problem s python-can bibliotekom koju sam namjeravao koristiti, a koja ne podržava ISO-TP protokol povrh kojeg radi UDS. Vođen tim problemom, čitao sam kod iz linux jezgre vezan uz socketcan, jer sve mogućnosti nisu u potpunosti dokumentirane. Uz can-isotp modul jezgre, linux podržava CAN sockete s ISO-TP protokolom te bi idealno bilo kada bi python-can biblioteka njih koristila. S obzirom na to da ne podržava navedene sockete, krenuo sam pisati vlastiti omotač oko ugrađenog

Python socket modula. U međuvremenu sam naišao na drugu Python biblioteku can-isotp koja se direktno može koristiti s python-can bibliotekom te implementira ISO-TP unutar Pythona povrh običnih CAN socketa. Kako bih uštedio na vremenu i fokusirao se na CTF zadatke, krenut ću pisati kod za simulirane ECU-ove s pomoću navedenih biblioteka, a ako mi ostane vremena napraviti ću svoj fork python-can biblioteke i dodati podršku za ISO-TP sockete.

Lijep pozdrav,  
Lovro Grgurić Mileusnić

**Wednesday, June 26, 2024 at 04:16:01 Central European Summer Time**

---

**Subject:** [DIPLOMSKI IZVJEŠĆE] Lovro Grgurić Mileusnić  
**Date:** Monday, 1 April 2024 at 18:42:12 Central European Summer Time  
**From:** Lovro Grgurić-Mileusnić  
**To:** Stjepan Groš  
**Attachments:** lovro\_grguricmileusnic\_22\_03\_2024.pdf, lovro\_grguricmileusnic\_29\_03\_2024.pdf

Poštovani profesore,

Šaljem Vam izvješće i bilješke za prošli i prethodni tjedan. Ispričavam se zbog zakašnjenja, prethodni tjedan nisam uspio napraviti sve što sam htio zbog bolesti pa sam Vam odlučio poslati sve kad nadoknadim i zaokružim ovaj dio rada.

Prethodni tjedan sam nastavio pisati Docker network plugin (driver) kojim ću umrežavati containere koristeći virtualna CAN sučelja koja pruža Linux jezgra. Postoji već projekt koji to radi, međutim ima dosta grešaka, slabo je dokumentiran i ništa ne sakriva od korisnika. Prvom polovicom tjedna čitao sam o network namespaceovima te paralelno programirao i proučavao postojeće implementacije više vrsta Docker pluginova s obzirom na to da dokumentacija za njihovo pisanje nije potpuno ažurna i nije na jednom mjestu. Drugu polovicu tjedna nisam radio zbog bolesti.

Tijekom prethodnog tjedna napisao sam omotavajući kod oko ip i cangw programa koje plugin koristi za stvaranje i povezivanje sučelja. Napisao sam dva načina rada plugina. Prvi pretpostavljeni način funkcionira kao i već spomenuti postojeći plugin te povezuje svaki container sa svakim s pomoću cangw pravila, što rezultira u velikom broju pravila ( $N$  povrh  $2 * 2$  pravila). Drugi način stvara vcan sučelje koje služi kao sabirnica te povezuje svaki container na to sučelje, što rezultira u  $2*N$  cangw pravila. Moja pretpostavka je da bi drugi način davao konzistentniji redoslijed poruka između containera, međutim za njegovo korištenje potrebno je ponovno učitati can\_gw modul jezgre s promijenjenim max\_hops parametrom. Napisao sam skripte za instalaciju i deinstalaciju plugina kao Systemd servisa te sam testirao integraciju s docker composeom. Uz klasični CAN (2.0A i 2.0B), dodao sam podršku za CAN FD te skrivanje svih stvorenih sučelja i cangw pravila unutar zasebnog network namespacea. Krajem tjedna i tijekom vikenda prisjetio sam se detalja oko CAN-a, CAN FD-a, ISO-TP-a, UDS-a, XCP-a te sam proučio can.h kako bih znao na što obratiti pažnju kod pisanja koda za simulirane ECU-ove.

Repozitorij u kojem se nalazi plugin:

<https://github.com/lgrguricmileusnic/dockercan>

Ovaj tjedan krenut ću s pisanjem predložaka koda koji pokrivaju navedene protokole, a u koje se može umetnuti konkretna implementacija simuliranog ECU-a.

Lijep pozdrav,

Lovro Grgurić Mileusnić

---

**Wednesday, June 26, 2024 at 04:16:01 Central European Summer Time**

---

**Subject:** [DIPLOMSKI IZVJEŠĆE] Lovro Grgurić Mileusnić  
**Date:** Saturday, 16 March 2024 at 12:38:01 Central European Standard Time  
**From:** Lovro Grgurić-Mileusnić  
**To:** Stjepan Groš

Poštovani profesore,

U ponedjeljak sam uspio umrežiti docker containere pomoću alata cannelloni i testirao komunikaciju preko "gateway" containera koji bi služio za filtriranje poruka između sabirnica. Ovo je sigurna opcija, ali sam htio pokušati napisati docker network driver koji će raditi na istom principu kao can4docker, ali biti skriveniji korisniku. Mislim da je to ispravniji način umrežavanja containera koji se direktno može uklopiti u docker compose.

Od utorka do petka sam proučavao libnetwork dokumentaciju o implementaciji drivera, prisjetio se jezika Go te pisao sam driver. Koristim Go obzirom da docker nudi službeni SDK za pisanje network driver-a u tom jeziku. Kod sam stavio u zaseban [repozitorij](#) i dodao ga kao podmodul [repozitoriju](#) sa svim materijalima vezanim za diplomski rad.

Pokušat ću osposobiti driver do kraja vikenda ili početkom idućeg tjedna. Dalje nastavljam na pisanje koda koji će zapravo komunicirati preko virtualnog CAN-a.

Lijep pozdrav,

Lovro Grgurić Mileusnić

---

**Wednesday, June 26, 2024 at 04:16:01 Central European Summer Time**

---

**Subject:** [DIPLOMSKI IZVJEŠĆE] Lovro Grgurić Mileusnić  
**Date:** Monday, 11 March 2024 at 14:18:01 Central European Standard Time  
**From:** Lovro Grgurić-Mileusnić  
**To:** Stjepan Groš  
**Attachments:** lovro\_grguricmileusnic\_08\_03\_2023.pdf

Poštovani profesore,

U prethodnom tjednu sam nastavio testirati prednosti i mane različitih arhitektura. Isprobao sam cannelloni za stvaranje TCP ili UDP tunela, obzirom da usmjeravanje CAN poruka pomoću cangw-a u ovom slučaju zahtjeva promjenu parametara can\_gw modula jezgre, što bi moglo prouzročiti probleme kasnije. Probao sam koristiti broadcast adrese kod definiranja UDP tunela kako bi simulirao sabirnicu, ali kod generiranja velike količine prometa dolazi do gubitka ili promjene poretka paketa. Još uvijek je moguće koristiti TCP tunele kako sam skicirao u bilješkama 12.1. te mi je to sigurna opcija. Još namjeravam probati napisati svoj docker network driver po uzoru na can4docker, gdje će onda svaka docker mreža biti jedna sabirnica. Implementacija can4docker drivera ima određene specifičnosti koje nisu idealne za ovu primjenu. Do kraja tjedna namjeravam biti gotov s povezivanjem containera kako bi mogao krenuti na osmišljanje CTF zadataka i njihovo kodiranje.

Ispričavam se na kasno poslanim bilješkama.

Lijep pozdrav,  
Lovro Grgurić Mileusnić

**Wednesday, June 26, 2024 at 04:16:01 Central European Summer Time**

---

**Subject:** [DIPLOMSKI ZADATAK] Lovro Grgurić Mileusnić  
**Date:** Sunday, 18 February 2024 at 14:29:18 Central European Standard Time  
**From:** Lovro Grgurić-Mileusnić  
**To:** Stjepan Groš

Poštovani profesore,

Na prošlom sastanku smo se dogovorili da Vam se javim nakon MI, kako bi se dogovorili oko zadatka za diplomski. Za sada smo okvirno bili rekli da bi trebalo napraviti pregled stanja kibernetičke sigurnosti u automobilske industriji te uz to napraviti i opisati modularni okvir za CTF-ove/edukacijsku platformu te pomoću njega stvoriti određeni broj izazova. Službeni rok za predaju zadatka u sustav je ovaj petak 23.2.

Lijep pozdrav,  
Lovro Grgurić Mileusnić

---

**Šalje:** Lovro Grgurić-Mileusnić  
**Poslano:** 14. veljače 2024. 19:10  
**Prima:** Stjepan Groš <[Stjepan.Gros@fer.hr](mailto:Stjepan.Gros@fer.hr)>  
**Predmet:** [IZVJEŠĆE PROJEKT] Lovro Grgurić Mileusnić

Poštovani profesore,

Na sastanku prije ispita smo se dogovorili da dodatno razradim moguće izvedbe simulatora i tehničke detalje oko vcan-a i vxcan-a.  
Razradio sam dvije opcije:

- svaki ECU u zasebnom containeru
- cijeli simulator u jednom containeru, svaki ECU zaseban proces

Tijekom izrade PoC-a za prvu opciju susreo sam se s nekoliko problema te ih nisam još uspio riješiti. Mislim da mi trenutni pristup nije dobar, ali imam još nekoliko načina za isprobati. Druga opcija je daleko jednostavnija po pitanju "umrežavanja" tako da PoC nisam radio.

Uz to, našao sam jedan poprilično loše dokumentirani docker network plugin "can4docker" i njegov poboljšani fork "docker-vxcan". Nisam znao što je to docker network plugin, tako da sam i to dodatno istražio. Navedena dva plugina stvaraju nešto jako slično onome što tražim i potpuno su integrirani u docker compose. Nakon instalacije plugina (jedna docker naredba) i odgovarajuće konfiguracije unutar compose.yml te pokretanja composea, automatski se stvara virtualna CAN mreža. Nedostatak je što su oba plugina puna bugova te što je mreža koju stvore potpuno transparentna potencijalnom sudioniku CTF-a. Još neke probleme sam zapisao u bilješkama.

Docker network plugini mi se čine kao ispravan način za umrežavanje containera, zbog integracije s compose-om, a implementiraju se jednostavno kao lokalni HTTP server koji odgovara na zahtjeve docker daemona. Mislim da je to dobra alternativa pisanju bash skripti ili programa s istom svrhom.

Lijep pozdrav,  
Lovro Grgurić Mileusnić

---

**Wednesday, June 26, 2024 at 04:16:01 Central European Summer Time**

---

**Subject:** Re: [DIPLOMSKI PROJEKT i IZVJEŠĆE] Bilješke uz izvješće i dogovor oko implementacije  
**Date:** Sunday, 21 January 2024 at 10:00:35 Central European Standard Time  
**From:** Lovro Grgurić-Mileusnić  
**To:** Stjepan Groš

Poštovani profesore,

Odgovara mi sastanak u utorak u 10 sati.

Lijep pozdrav,  
Lovro Grgurić Mileusnić

---

On Jan 21, 2024 at 8:49 AM, <[Stjepan Groš](#)> wrote:

Kolega,



ja sam prošli tjedan (i tjedan prije toga) bio bolestan. Sad sam ponovo OK pa gledam mailove.

Sastanak bi svakako mogli dogovoriti. Odgovara li vam možda utorak u 10 sati?

SG

On 15. 01. 2024. 11:44, Lovro Grgurić-Mileusnić wrote:

Poštovani profesore,

U privitku su bilješke koje sam zaboravio poslati uz izvješće.

Na posljednjem sastanku smo se dogovorili da razradim moguće načine implementacije simulatora te da Vam se javim kako bi ih skupa prokomentirali. U bilješkama i izvješću su skice i razrada mogućih načina implementiranja.

Ako imate vremena da se sastanemo, odgovara mi bilo koje vrijeme ovaj tjedan osim utorka i petka poslije 14 sati.

Lijep pozdrav,  
Lovro Grgurić Mileusnić

---

**From:** Lovro Grgurić-Mileusnić <[Lovro.Grguric-Mileusnic@fer.hr](mailto:Lovro.Grguric-Mileusnic@fer.hr)>

**Date:** Monday, 15 January 2024 at 11:23

**To:** Stjepan Groš <[Stjepan.Gros@fer.hr](mailto:Stjepan.Gros@fer.hr)>

**Subject:** [IZVJEŠĆE PROJEKT] Lovro Grgurić Mileusnić

Poštovani profesore,

Sukladno našem razgovoru, potražio sam implementacije otvorenog koda automobilskih OS-ova, infotainmenta i digitalnih ploča s instrumentima. Pronašao sam nekoliko OS-ova, od kojih se najviše ističu Android Automotive OS i Automotive Grade Linux. Međutim mislim da nema smisla kompajlirati i pokretati cijeli OS samo radi vizualizacije tijekom napadanja simulatora te sam našao nekoliko GUI-a iz gore navedenih OS-ova, koji se mogu samostalno pokretati. Najprikladnija mi se čini ploča s instrumentima iz AGL projekta napisana u Flutteru, s obzirom na to da ima otvoreni KUKSA server za upravljanje GUI-jem.

Preuzeo sam i isprobao CANdevtools alat koji sam Vam spomenuo na sastanku. Alat je zapravo korisničko sučelje izgrađeno na Qt-ovoj CAN biblioteci te omogućuje komunikaciju između više hardverskih i virtualnih CAN sučelja, filtriranje i interpretiranje CAN signala korištenjem dbc datoteka. Uz to, ima komponentu koja omogućava izgradnju GUI-ja u QML-u, koja onda može reagirati na CAN promet grafički ili ga modificirati. Nedostatak alata u kontekstu projekta je što je napravljen za sekvencijalnu obradu i modifikaciju CAN prometa te debugiranje istog. Koristiti ga kao CAN simulator imalo bi nedostatke s obzirom na to da unutar alata ne postoji CAN sabirnica, već su sve veze između CAN uređaja 1:1.

U bilješkama sam razradio i skicirao tri načina implementacije simulatora. Mislim da je najčišća prva izvedba koja ne koristi Docker, već svaki ECU emulira zasebnim procesom ili dretvom. Ako bih koristio Docker, opcija s vxcan-om mi se čini najispravnija. Uz to, razmislio sam o načinu na kojem bi se mogla implementirati modularna logika ECU-ova u različitim jezicima te o obliku .yaml datoteke za konfiguraciju mreže uređaja koja će biti simulirana.

Vezano za izvještavanje, nisam bio primijetio da imamo rok 5.1. za poslati novo izvješće tako da Vam tada nisam ništa poslao te ću to nadoknaditi ovaj tjedan.

U prethodna dva tjedna sam se potrudio nadoknaditi zaostatke od prije blagdana.

Tijekom idućeg tjedna ću se posvetiti implementaciji simulatora.

Lijep pozdrav,  
Lovro Grgurić Mileusnić

--

associate professor Stjepan Groš, Ph.D.

[Laboratory for Information Security and Privacy](#)

[Faculty of Electrical Engineering and Computing](#)

[University of Zagreb](#)

Tel: +385 (0)1 6129 943

Mob: +385 (0)91 6454 982

Fax: +385 (0)1 6129 653

E-mail: [stjepan.gros@fer.hr](mailto:stjepan.gros@fer.hr)

Web: <https://www.fer.unizg.hr/stjepan.gros>

**Wednesday, June 26, 2024 at 04:16:01 Central European Summer Time**

---

**Subject:** Re: Diplomski projekt pitanja

**Date:** Monday, 18 December 2023 at 11:06:36 Central European Standard Time

**From:** Lovro Grgurić-Mileusnić

**To:** Stjepan Groš

Odgovara mi četvrtak. Greškom sam Vam prvi mail poslao s poslovne adrese.

Nisam Vam poslao izvješće za prethodni tjedan jer nisam stigao raditi na projektu. Cijeli tjedan mi je bio poprilično kaotičan zbog selidbe u drugi stan te se nisam uspio dobro organizirati. Nadoknadit ću to tijekom prvog tjedna iduće godine.

Lijep pozdrav,  
Lovro Grgurić Mileusnić

On Dec 18, 2023 at 10:31 AM, <[Stjepan.Gros@fer.hr](mailto:Stjepan.Gros@fer.hr)> wrote:

You don't often get email from [stjepan.gros@fer.hr](mailto:stjepan.gros@fer.hr). [Learn why this is important](#)

**Caution:** EXTERNAL EMAIL: Do not click any links or open any attachments unless you trust the sender and know the content is safe.

Bi li vam odgovaralo da se nađemo u četvrtak u 13:40?

SG

On 12. 12. 2023. 12:01, Lovro Grgurić Mileusnić INTERN wrote:

Poštovani profesore,

Na početku akademske godine smo razgovarali o nekoj vrsti automobilske CTF/edukacijske platforme kao okvirni smjer za diplomski.

Obzirom da je krenuo drugi ciklus semestra, htio bih se s Vama konzultirati oko detalja i konačnom cilju za diplomski projekt.

Dosadašnji cilj je bio saznati što bi jedna takva platforma trebala uključivati te istražiti alate i tehnologije koji bi mogli biti od koristi u implementaciji.

Lijep pozdrav,  
Lovro Grgurić Mileusnić

--

associate professor Stjepan Groš, Ph.D.

[Laboratory for Information Security and Privacy](#)  
[Faculty of Electrical Engineering and Computing](#)  
[University of Zagreb](#)

Tel: +385 (0)1 6129 943

Mob: +385 (0)91 6454 982

Fax: +385 (0)1 6129 653

E-mail: [stjepan.gros@fer.hr](mailto:stjepan.gros@fer.hr)

Web: <https://www.fer.unizg.hr/stjepan.gros>

**Wednesday, June 26, 2024 at 04:16:01 Central European Summer Time**

---

**Subject:** [IZVJEŠĆE PROJEKT] Lovro Grgurić Mileusnić  
**Date:** Sunday, 10 December 2023 at 18:02:55 Central European Standard Time  
**From:** Lovro Grgurić-Mileusnić  
**To:** Stjepan Groš  
**Attachments:** lovro\_grguricmileusnic\_08\_12\_2023.pdf

Poštovani profesore,

U prethodnom tjednu sam isprobao socketcan biblioteke za Python, C i Go te pročitao jedan rad koji klasificira oko 160 kibernetičkih napada u automobilske industriji, što bi mi moglo biti korisno kod osmišljanja izazova za edukacijsku platformu. Uz to, pronašao sam još nekoliko alata koji bi mi mogli biti od koristi.

Neizravno vezano za diplomski projekt, uskoro ću imati više praktičnog iskustva s fuzzy testiranjem ECU-ova, obzirom da mi je rad na razvoju fuzzera nova odgovornost na radnom mjestu.

Ispričavam se što Vam kasno šaljem izvješće.

Lijep pozdrav,  
Lovro Grgurić Mileusnić

**Wednesday, June 26, 2024 at 04:16:01 Central European Summer Time**

---

**Subject:** Re: [DIPLOMSKI PROJEKT I IZVJEŠĆE] Bilješke uz izvješće i dogovor oko implementacije

**Date:** Sunday, 21 January 2024 at 08:49:25 Central European Standard Time

**From:** Stjepan Groš

**To:** Lovro Grgurić-Mileusnić

Kolega,

ja sam prošli tjedan (i tjedan prije toga) bio bolestan. Sad sam ponovo OK pa gledam mailove.

Sastanak bi svakako mogli dogovoriti. Odgovara li vam možda utorak u 10 sati?

SG

On 15. 01. 2024. 11:44, Lovro Grgurić-Mileusnić wrote:

Poštovani profesore,

U privitku su bilješke koje sam zaboravio poslati uz izvješće.

Na posljednjem sastanku smo se dogovorili da razradim moguće načine implementacije simulatora te da Vam se javim kako bi ih skupa prokomentirali.  
U bilješkama i izvješću su skice i razrada mogućih načina implementiranja.

Ako imate vremena da se sastanemo, odgovara mi bilo koje vrijeme ovaj tjedan osim utorka i petka poslije 14 sati.

Lijep pozdrav,  
Lovro Grgurić Mileusnić

---

**From:** Lovro Grgurić-Mileusnić <[Lovro.Grguric-Mileusnic@fer.hr](mailto:Lovro.Grguric-Mileusnic@fer.hr)>

**Date:** Monday, 15 January 2024 at 11:23

**To:** Stjepan Groš <[Stjepan.Gros@fer.hr](mailto:Stjepan.Gros@fer.hr)>

**Subject:** [IZVJEŠĆE PROJEKT] Lovro Grgurić Mileusnić

Poštovani profesore,

Sukladno našem razgovoru, potražio sam implementacije otvorenog koda automobilskih OS-ova, infotainmenta i digitalnih ploča s instrumentima.

Pronašao sam nekoliko OS-ova, od kojih se najviše ističu Android Automotive OS i Automotive Grade Linux. Međutim mislim da nema smisla kompajlirati i pokretati cijeli OS samo radi vizualizacije tijekom napadanja simulatora te sam našao nekoliko GUI-a iz gore navedenih OS-ova, koji se mogu samostalno pokretati. Najprikladnija mi se čini ploča s instrumentima iz AGL projekta napisana u Flutteru, s obzirom na to da ima otvoreni KUKSA server za upravljanje GUI-jem.

Preuzeo sam i isprobao CANdevtools alat koji sam Vam spomenuo na sastanku. Alat je zapravo korisničko sučelje izgrađeno na Qt-ovoj CAN biblioteci te omogućuje komunikaciju između više hardverskih i virtualnih CAN sučelja, filtriranje i interpretiranje CAN signala korištenjem dbc datoteka. Uz to, ima komponentu koja omogućava izgradnju GUI-ja u QML-u, koja onda može reagirati na CAN promet grafički ili ga modificirati. Nedostatak alata u kontekstu projekta je što je napravljen za sekvencijalnu obradu i modifikaciju CAN prometa te debugiranje istog. Koristiti ga kao CAN simulator imalo bi nedostatke s obzirom na to da unutar alata ne postoji CAN sabirnica, već su sve veze između CAN uređaja 1:1.

U bilješkama sam razradio i skicirao tri načina implementacije simulatora. Mislim da je najčišća prva izvedba koja ne koristi Docker, već svaki ECU emulira zasebnim procesom ili dretvom. Ako bih koristio Docker, opcija s vxcan-om mi se čini najispravnija. Uz to, razmislio sam o načinu na kojem bi se mogla implementirati modularna logika ECU-ova u različitim jezicima te o obliku .yaml datoteke za konfiguraciju mreže uređaja koja će biti simulirana.

Vezano za izvještavanje, nisam bio primijetio da imamo rok 5.1. za poslati novo izvješće tako da Vam tada nisam ništa poslao te ću to nadoknaditi ovaj tjedan.

U prethodna dva tjedna sam se potrudio nadoknaditi zaostatke od prije blagdana. Tijekom idućeg tjedna ću se posvetiti implementaciji simulatora.

Lijep pozdrav,  
Lovro Grgurić Mileusnić

--

associate professor Stjepan Groš, Ph.D.  
[Laboratory for Information Security and Privacy](#)  
[Faculty of Electrical Engineering and Computing](#)  
[University of Zagreb](#)  
Tel: +385 (0)1 6129 943  
Mob: +385 (0)91 6454 982  
Fax: +385 (0)1 6129 653  
E-mail: [stjepan.gros@fer.hr](mailto:stjepan.gros@fer.hr)  
Web: <https://www.fer.unizg.hr/stjepan.gros>

**Wednesday, June 26, 2024 at 04:16:01 Central European Summer Time**

---

**Subject:** [IZVJEŠĆE PROJEKT] Lovro Grgurić Mileusnić  
**Date:** Friday, 3 November 2023 at 01:01:08 Central European Standard Time  
**From:** Lovro Grgurić-Mileusnić  
**To:** Stjepan Groš

**Attachments:** lovro\_grguricmileusnic\_20\_10\_2023.pdf, lovro\_grguricmileusnic\_03\_11\_2023.pdf

Poštovani profesore,

Prošao sam kroz simulatore koje ste mi poslali i kroz još nekoliko alternativa. Uz to, riješio sam izazove vezane uz ICSim na Blockharbourovoj VSEC platformi.

Najbolji API za “nakačiti” emulirani, simulirani ili stvarni ECU kroz Python i C++ imaju Carla i AirSim, gdje Carla ima više mogućnosti.

Najviše mogućnosti definitivno nudi BeamNG, koji nažalost nije besplatan (oko 25 EUR).

“Modovi” za BeamNG pišu se u jeziku Lua i omogućuju upravljanje s puno više različitih vizualnih indikatora u odnosu na ostale simulatore.

S druge strane, nisam siguran je li potrebno spajati se na simulatore koji imaju toliko mogućnosti koje ne bi koristili.

Ako tražimo samo vizualne pokazatelje kod hakiranja možda bi jednostavan GUI bio bolje rješenje?

Takav pristup koristi ICSim koji prikazuje samo neke elemente kontrolne ploče (brzinomjer, pokazivači smjera, stanje vrata).

U prilogu su i bilješke od prvog tjedna s ispravljenim naslovom.

Lijep pozdrav,

Lovro Grgurić Mileusnić