FAKULTET ELEKTROTEHNIKE, STROJARSTVA I BRODOGRADNJE SPLIT

Sigurnost bežičnih medicinskih uređaja

Sigurnost bežičnih mreža - seminarski rad

Ivan Lukšić
Bruno Grbavac

Diplomski studij računarstva (250)
Akademska godina 2022./23.

Sadržaj

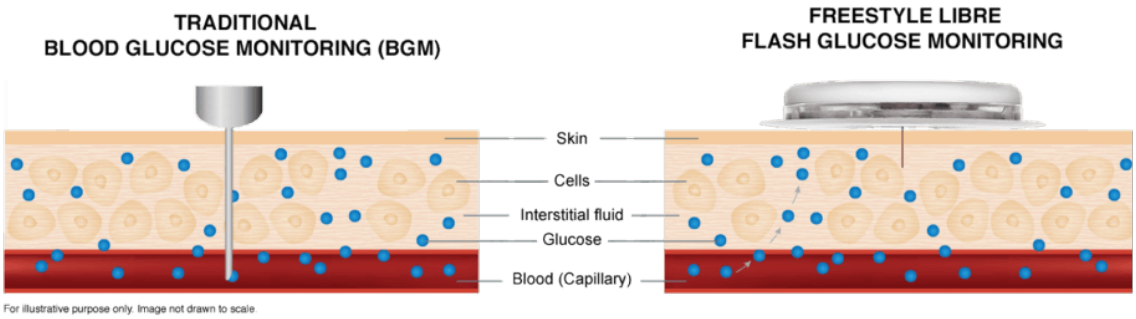
1 Uvod

Kroz ovaj seminar ćemo ispitivati sigurnost uređaja za bežično očitavanje mjerenja glukoze. **Freestyle Libre verzija 1** je uređaj kojeg dijabetičari u Hrvatskoj mogu dobiti preko Hrvatskog zavoda za zdravstveno osiguranje, pa ima smisla da taj uređaj testiramo. Testiranje se odnosi na bilo kakav oblik promjenu stanja uređaja, koje se mogu odraziti na korisnika (dijabetičara), van predviđenih mogućnosti. Za testiranje ćemo koristiti **proxmark3**, koji je najreferentniji uređaj za testiranje i manipuliranje RFID i NFC komunikacije. U nastavku seminara ćemo objasniti okruženje i njegovo postavljanje, elaborirati testiranja i postaviti u sigurnosni kontekst rezultate spomenutog testiranja.

2 Freestyle Libre 1

Flash Glucose Monitoring (FGM) omogućuje mjerenje razine glukoze u krvi bez kontinuiranog bockanja koje je do pojave ovakvih uređaja bilo ustaljeno. FGM uređaji kontinuirano (s intervalnim razmakom od nekoliko minuta, iako postoje i CGM (*eng. continous*) uređaji koji konstantno mjere razinu glukoze) očitavaju razinu glukoze i stanja pohranjuju u memoriju, odakle se ona kasnije mogu očitati handheld čitačem ili mobilnom aplikacijom. [2]

Vrijedi napomenuti da mjerenje bockanjem i FGM mjerenja uglavnom neće proizvesti jednaka očitanja jer se mjerenja senzorom izvode na **međustaničnoj tekućini** (*eng. ISF - interstitial fluid*), koja okružuje stanice u tankom sloju pod kožom. Pokazalo se kako mjerenja na međustaničnoj tekućini kasne oko 2.1 minute kod djece i 2.4 minute za odrasle u odnosu na mjerenja temeljena na krvi.[2]

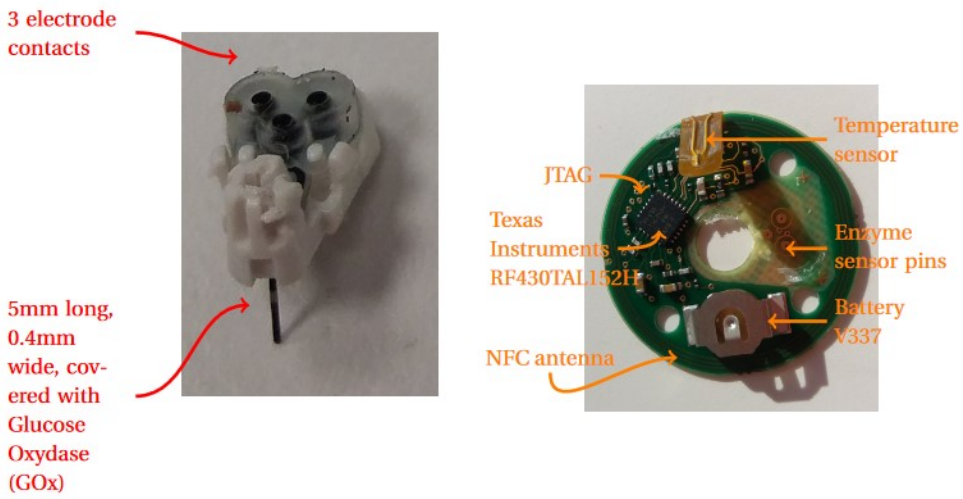


Slika 1: FGM mjerenje temeljeno na razini glukoze u ISF [2]

Sam uređaj je zbog licenci propisanih zdravstvenim sustavom softverski ograničen na uporabu od 14 dana nakon aktivacije. Senzor se očitava uređajem ili mobitelom sa udaljenosti od 1cm do 4cm, te je vodootporan na dubini do 1m.

Sam uređaj se prije korištenja sastoji od dva dijela, od aplikatora sa električnom pločom i senzora za mjerenje enzima koji dolazi u sterilnom pakiranju.

Senzor za mjerenje koncentracije enzima sastoji se od 3 elektrode (radna, referentna i pomoćna) te kontakata. Sama nit koja ulazi pod kožu i u kontaktu je s međustaničnom tekućinom prekrivena je **glukozom-oksidazom (GOx)** te polupropusnom membranom. Reakcija navedenog spoja s ISF-om proizvodi električni signal kojeg senzor detektira i obrađuje - sam senzor dolazi kalibriran od strane tvornice.[1]



Slika 2: Senzor za mjerenje glukoze [1]

Električna (tiskana) pločica sastoji se od **Texas Instruments čipa RF430 TAL152H TI 79I CKK8 F** koji je zadužen za upravljanje NFC naredbama, senzora temperature (bitnog za detekciju spajanja uređaja na čovjeka kao i za prilagođavanje mjerenja GOx senzora ovisno o gradijentu temperature između vanjskog zraka i kože kojeg računa pomoću 2 termistora), **NFC antene** koja šalje signal Texas Instruments čipu te **baterije** koja je tu prvenstveno radi povećavanja preciznosti mjerenja.[1]

3 Proxmark 3 RDV 4.01

Proxmark 3 RDV 4.01 je uređaj višestruke namjene u području RFID tehnologija te omogućuje čitanje, pisanje, analizu, prisluškivanje, replikaciju, emulaciju, modulaciju i demodulaciju, dekodiranje i enkodiranje, dekripciju i enkripciju u frekvencijskom području od 125 kHz do 13,56 MHz.[3]

Proxmark 3 podržava tri različita moda rada - sniffing mod, mod za emulaciju kartice i mod za čitanje. Sam uređaj sastoji se od SAM7S512 procesora, 256kB SPI Flash memorije te podržava vanjsku memoriju pri 2Mb/s, visokofrekvencijske antene koja radi pri 13.56Mhz i nisko-frekvencijske na pojasu od 125 kHz do 134 kHz. Uređaj sadrži sučelje za SIM i pametne kartice kao i multifunkcionalni ekspanzijski port te podržava USB 2.0.

Slika 3: Proxmark 3 RDV4.01 [3]

3.1 Postavljanje okruženja za rad s Proxmarkom

Za našu primjenu s Proxmarkom je potrebno komunicirati pomoću **Proxmark 3** klijentskog okruženja koje je mnogo manje zastupljeno u odnosu na preporučeno i najviše podržano od strane zajednice - Iceman okruženje.[4] Za instalaciju potrebno je pratiti sljedeće korake:

1. Preuzeti instalacijski paket "Proxspace-master.zip" s `https://github.com/Gator96100/ProxSpace/archive/master.zip`.
2. Sinkronizirati preuzeti paket s `https://github.com/Proxmark/proxmark3` repozitorijem.
3. Preimenovati nastali ***/proxmark3*** folder u ***/pm3***.
4. Testirati konfiguraciju pokretanjem ***"runme.bat"*** datoteke nakon čega se otvara Minimalist GNU konzolno sučelje.
5. Pokretanjem naredbe ***"make clean && make all"*** u otvorenom sučelju buildaju se izvršne datoteke i firmware za proxmark.
6. Otvoriti Upravitelj uređaja (device manager) te desnim klikom na Proxmark odabrati opciju "Ažuriraj upravljački program" (*eng. "update driver"*).

U slučaju da nakon prethodno objašnjenje instalacije dođe do problema, moguće ih je pokušati riješiti flashanjem Proxmarka na najnoviju **verziju firmwarea**.

1. Flasha se bootrom korištenjem sljedeće naredbe - ***./client/flasher comx -b ./bootrom/obj/bootrom.elf*** gdje je comx oznaka porta vidljiva u Upravitelju uređaja (npr. COM4)
2. Potrebno je isključiti proxmark iz računala jer je moguće da dođe do promjene COM porta, te da brickate uređaj :).
3. Uključiti uređaj u računalo te provjeriti COM port u Upravitelju uređaja.
4. Flashati firmware koristeći sljedeću naredbu - ***./client/flasher comx ./armsrc/obj/fullimage.elf*** gdje je comx oznaka porta vidljiva u Upravitelju uređaja (npr. COM4).

4 Teorijski mogući napadi

Kako bi zaključili koji su to možebitni sigurnosni propusti Freestyle Libre-a potrebno je sagledati kako se podaci o mjerenjima pohranjuju i razmjenjuju s čitačem ili mobilnom aplikacijom.

4.1 Struktura memorije Freestyle Librea [1]

RF 430 TAL čip nije javno dostupan no znamo da uz MSP430 RISC mikrokontroler, Tag-It HF-transponder koji podržava **NFC 15693** na 13,56 MHz sadrži i **2 KB Feroelektričnog RAM-a** - nevolatilnu memoriju za pohranu programskog koda i samih korisničkih podataka.

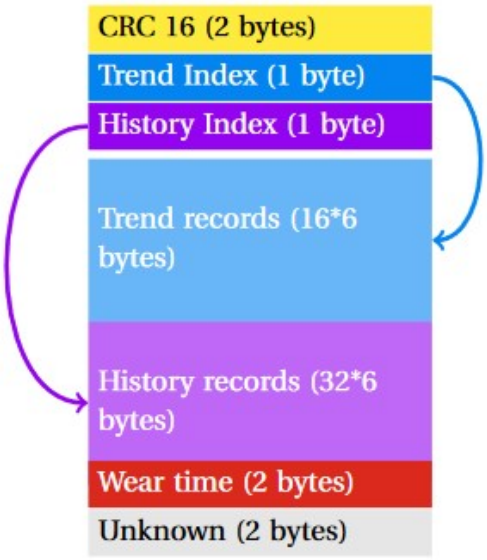
Sama FRAM memorija podijeljena je na 5 sektora - **aktivacijske blokove**, **mjerenja razine glukoze**, **zapis o regiji** senzora, **naredbe** te **podnožje**.

Prva dva okteta aktivacijske sekcije FRAM-a ista su kao i kod ostalih sekcija te sadrže **cikličku provjeru ispravnosti sekcije (CRC16)**. Sadržaj iduća dva okteta je nepoznat. Oktet F864 sadrži **"Stage of Life"** vrijednost koja poprima 5 različitih vrijednosti, oktet F865 predstavlja **"Activity"** flag - 0 za ugašen te 1 za aktivan senzor. Posljednja 2 okteta sekcije mijenjaju vrijednost u procesu aktivacije senzora, no ne zna im se točno značenje.

Vrijednost	Stage of Life
1	spreman za aktivaciju
2	trenutno se aktivira
3	senzor je operabilan
5	senzor je istekao
6	greška

Tablica 1: Enumerator "Stage of Life" vrijednosti.

Kod sekcije sa zapisima o mjerenjima razine glukoze nakon 2 okteta CRC16 zaštite sekcije, slijede oktet **indeksa trenda** F87A koji označava trenutan trend zapis u tablici trendova te F87B - oktet **indeksa povijesnih zapisa** koji označava trenutni *"history"* zapis u tablici istih. Nakon slijede već spomenuta **tablica trendova** koja sadrži 16 zapisa po 6 okteta koji predstavljaju mjerenja posljednjih 16 minuta (F87C-F8DB), te **tablica povijesnih zapisa** sa 32 6-oktetna zapisa koja predstavljaju posljednjih 32 16-minutna trenda to jest stanje pacijenta u posljednjih cca. 8,5 sati. U ovoj sekciji zatim slijede 2 okteta koja predstavljaju **"Wear Time"** - broj minuta od aktivacije uređaja i 2 okteta čije se značenje ne zna.



Slika 4: Sekcija s zapsima o mjerenjima raziine glukoze. [1]

Sekcija regije senzora (F9A0 - F9B7) sadrži 2 2-oktetna zapisa - CRC16 zaštitu valjanosti sekcije, **zapis regije** te 20 okteta čije je značenje nepoznato.

Vrijednost	Geografska regija
01	Europska unija/ Ujedinjeno kraljevstvo
02	Sjedinjene Američke Države - 10 dnevni senzor
08	Izrael

Tablica 2: Enumerator za zapis regije.

Sekcija naredbi sastoji se od koda naredbi uređaja u oktetima od F9BA do FFA3, te 2 tablice - onu **omogućenih** (FFA4-FFAF) i onu **onemogućenih** (FFB0-FFC7) naredbi. Obje tablice sadrže **listu naredbi** čiji se član sastoji od - adrese naredbe u kodu i njenog NFC identifikatora po 2 okteta.

Footer sekcija sadrži podatke poput tablice prekida procesora.

4.2 Napadi [1]

Glavni sigurnosni nedostatak ovog uređaja je postojanje **naredbe koja otključava mogućnost pisanja** nad blokovima 0x00-0xf3. Naime, sam čip omogućava čitanje određenih blokova kako bi se stanje pacijenta moglo očitati od strane doktora ili drugih pružatelja zdravstvene skrbi ili pomoći, no pisanje na čip trebalo bi biti dopušteno samo službenoj aplikaciji.

Naime, probamo li pisati u blok 0x03 bez navedene naredbe - nailazimo na zabranu pisanja.

```
proxmark3> hf 15 cmd write u 03 62 C2 00
  00 00 00 00 00
Tag returned Error 18: The specified block
is locked and its content cannot be changed.
```

Slika 5: Pokušaj pisanja bez otključavanja - neuspješno. [1]

Koristimo li potom **naredbu A4 uz tajnu lozinku**, moguće je izvršiti pisanje.

```
proxmark3> hf 15 cmd raw -c 02 XX 07
   ==CENSORED==
received 3 octets
00 78 F0
```

Slika 6: Otključavanje tajnom naredbom i lozinkom. [1]

```
proxmark3> hf 15 cmd write u 03 62 C2 00
 00 00 00 00 00
```

Slika 7: Pokušaj pisanja bez otključavanja - uspješno. [1]

4.2.1 Izmjena vremena isteka

Na hardverskom nivou ova se izmjena odnosi na polja "Wear Time" iz sekcije mjerenja glukoze (koje se povećava svaku minutu) te polje "Stage of life" iz sekcije za aktivaciju. Dosegne li "Wear Time" limit trajanja polje "Stage of life" se postavlja na vrijednost za uređaj koji je istekao. Softver aplikacije **"dumpa" NFC blokove 0x00 do 0x2a** te tako dobiveni "Wear Time" uspoređuje s limitom.

Najjednostavniji način produljenja trajanja uređaja stoga bi bio **izmjena "Wear Time-a"** što zahtjeva izmjenu zaštitnih CRC16 suma koja štiti tu sekciju ili **izmjenu "hard-code-ane"**

vrijednosti "wear-limita" za koju ne znamo odakle ju native library dohvaća.

4.2.2 Ponovno korištenje senzora kojem je istekao rok uporabe

Kako se mehanička ispravnost samog uređaja ne mijenja prelaskom propisanog roka trajanja, moguće je omogućiti valjanja mjerenja nakon isteka. Naime, rok je uveden putem medicinskih licenci koje granicu korištenja propisuju uzimajući u obzir zdravstvene faktore poput mogućnosti razvoja upale neispravnim apliciranjem senzora na npr. nečistu kožu itd..

Načelno je potrebno postaviti na nulu blokove 1 i 2, te urediti blok 0 tako da je **"Stage of Life" postavljen na 0x01 to jest na "to activate"**, **"Activity" flag postavljen na 0x00** te izračunat odgovarajući CRC16. Zatim postaviti sve blokove iz sekcije **mjerenja glukoze na nulu** (izračunati odgovarajući CRC za sekciju).

Kod ovakvog "napada" potrebno je pripaziti, u slučaju da se senzor želi koristiti s mobilnom aplikacijom, da uređaj **nije korišten na tom telefonu**, odnosno potrebno ga je izbrisati iz baze podataka - jer smo uređaj vratili na "Stage of Life" = "spreman za aktivaciju" te ga je potrebno ponovno postaviti kao novi uređaj.

4.2.3 Onemogućavanje senzora (ubijanje)

Ovo je možda najlakši i sigurnosno najopasniji napad jer može od korisnicima **onemogućiti praćenje stanja krvne slike do nabavke novog senzora** unutar sekunde.

Kao što je već spomenuto, svaka sekcija zaštićena je cikličkom zaštitom te će iz toga razloga **bilo kakva promjena** koja nije praćena ponovnim izračunom CRC16 učiniti senzor aplikacija prepozna kao neispravan - onemogući njegovo korištenje.

Drugi način je promjena vrijednosti polja **"Stage of Life" na 5** odnosno "senzor je istekao".

```
print('Blocks 1 and 2: zero')
core.console("hf 15 cmd write u 1 00 00
 ↪  00 00 00 00 00 00")
core.console("hf 15 cmd write u 2 00 00
 ↪  00 00 00 00 00 00")
print('Block 0: Kill StageOfLife=5 and
 ↪  Indicator=1 and CRC')
core.console("hf 15 cmd write u 0 3F 73
 ↪  B0 32 05 01 02 08")
```

Slika 8: Onemogućavanje senzora. [1]

4.2.4 Promjena regije senzora

Uređaj je moguće koristiti samo s odgovarajućom aplikacijom za tu regiju što može predstavljati izazov pri promjeni prebivališta ili pri nabavki uređaja zbog nedostupnosti u zemlji prebivanja. Nadalje, **različite regije propisuju različita ograničenja** na uređaj poput roka trajanja te vremena zagrijavanja (moguće mijenjati i na način na koji je predviđena izmjena "wear limit"-a) uređaja kod aktivacije.

Promjenom regije stoga se može produžiti rok trajanja, smanjiti vrijeme zagrijavanja te koristiti uređaj u državi u kojoj nije dobavljiv.

4.2.5 Promjena zapisa o razini glukoze

Izmjenom F87C-F99B vrijednosti moguće je korisniku prikazati **neispravne razine glukoze u krvi** te tako izravno utjecati na njegovo zdravstveno stanje u slučaju da vođen neispravnim mjerenjima pacijent kontrolira razine glukoze. Uz to je naravno potrebno pri svakoj izmjeni izračunati odgovarajući iznos zaštitne sume sekcije.

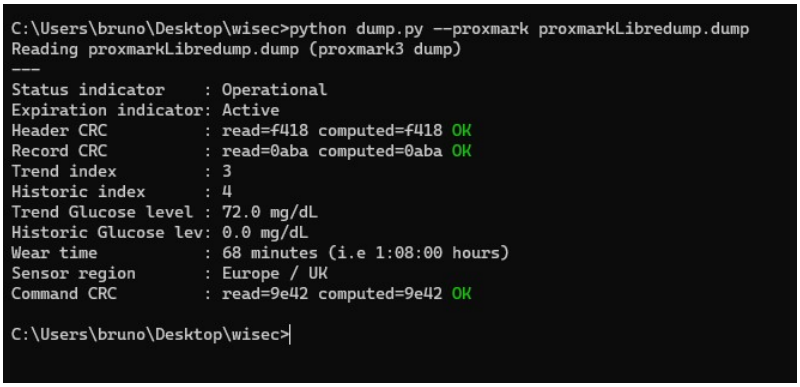
5 Rezultati seminara

Komandom '*hf 15 dumpmemory*' dobijemo izlist svih javno dostupnih polja i to u sljedećem formatu:

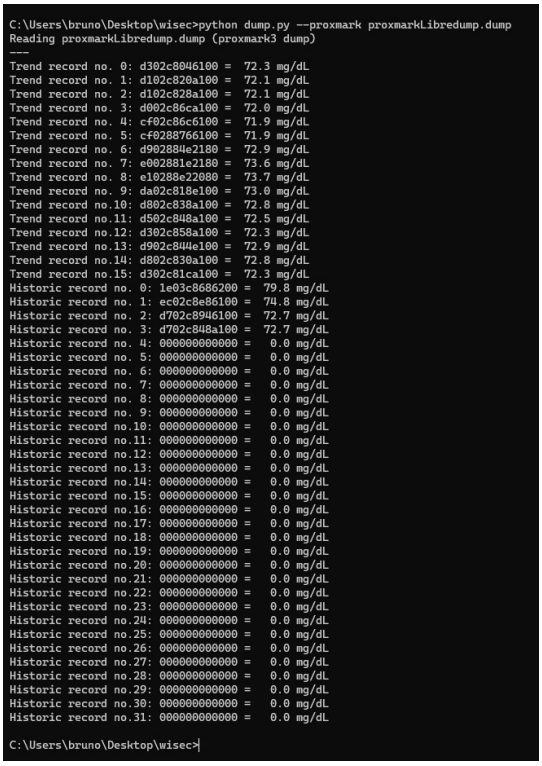
```
[=] [=]  block#    | data        |lck| ascii
[=] ----------+-----------------+---+----------
[=]    0/0x00  | E1  8D  90  5B  | 0 | ...[
[=]    1/0x01  | 51  04  13  54  | 0 | Q..T
[=]    2/0x02  | 00  00  00  00  | 0 | ....
[=]    3/0x03  | F6  94  02  0A  | 0 | ....
[=]    4/0x04  | 34  81  19  00  | 0 | 4
                        ...
```

Kao što vidimo svaki blok sadrži 8 heksadecimalnih znakova, a 244 blokova je javno dostupno, međutim to ne predstavlja neželjeno ponašanje, jer po dizajnu svatko može pročitati informacije o vrijednostima koje je senzor očitao. Ta značajka, iako se može tumačiti kao povreda privatnosti, je napravljena kako bi liječnici mogli očitati vrijednosti u potencijalno opasnim situacijama. Pomoću antene, moguće je pročitati te vrijednosti s udaljenosti do 10 cm.

Pokretanjem skripte navedene u [1] dobivamo formatiran i čitljiv ispis gore navdenog dumpa NFC blokova.



Slika 9: Prikaz dumpunih podataka.



Slika 10: Prikaz svih zapisa o razini glukoze iz dumpunih podataka.

Kako probijanje lozinke otključava manipuliranje senzorom na više načina, prvo smo se prihvatili otkrivanja koja se komanda koristi prilikom otključavanja senzora. Za to smo napravili lua skriptu koja šalje na senzor svaku moguću kombinaciju heksadecimalnih znamenki te smo analizirali povratne informacije. Primjer poslane komande i odgovora senzora:

```
hf 15 cmd raw -c 02 a8 07
received 4 octets
01 01 16 07
hf 15 cmd raw -c 02 a9 07
received 4 octets
01 01 16 07
hf 15 cmd raw -c 02 a0 07
card didn't respond
        ...
```

Za nekoliko kombinacija znakova kartica nije odgovorila te su to one komande zaštićene lozinkom. Iz literature smo zaključili što rade neke od tih komandi te nam je ostala jedna koja služi za otključavanje.

Sljedeći korak je pronalazak lozinke za senzor te nam je prvotna ideja bila nalik onoj za pronalazak komande za otključavanje. Kako se lozinka sastoji od 8 heksadecimalnih znamenki postoji $16^8 = 2^{32}$ mogućih kombinacija što u je nedostatno kontekstu sigurnosti u modernim sustavima, međutim pojavili su se problemi tokom brute force napada.

Prvi problem je relativno spor interface između proxmarka i senzora što proxmark šalje naredbu senzoru te čeka odgovor neko vrijeme koje je par redova veličine veće od vremena koje bi bilo potrebno da se izvršava na računalu.

Drugi problem na koji smo naišli je kako bi ostavili proxmark da pokušava sve mogućnosti da bi on prestao slati komande na izvršavanje nakon malo više od 2^{16} pokušaja te bi se trebao restartati prije ponovnog početka napada.

Zbog ta dva problema i vremena preostalog za završetak seminara smo zaključili da brute force napad nije moguće napraviti u nekom realnom vremenu kojeg imamo za seminar.

5.1 Propusti u našem radu

Vremenska ograničenost iskazala se kao nepremostiv nedostatak našeg izravnog, ali na kraju suviše naivnog pristupa.

Pribavljanje lozinke koja omogućuje pisanje na zaključane blokove uređaja može se iščitavati na dva mjesta, uzimajući u obzir da se upravo tajna lozinka korištena uz naredbe koristi pri samoj aktivaciji uređaja. Znajući to moguće je pozive (tokom aktivacije) s lozinkom pratiti na **SPI sabirnici** (osciloskopom) između procesora i NFC kontrolera samog uređaja ili iščitavajući **pozive android aplikacije prema NFC biblioteci**.

6 Primjenjivost modela u praksi

Da smo uspjeli dobiti lozinku na neki od gore nabrojanih načina, bi pomoću dvije komande, prve za otključavanje, druge koja proizvoljno mijenja bilo koji blok zaštićen CRC-om, mogli onesposobiti uređaj tako da dijabetičar ne može dobiti vrijednosti glukoze. To je potencijalna opasnost, pogotovo ako dijabetičar nije u mogućnosti izmjeriti vrijednosti glukoze u krvi ili nema zamjenski senzor pri ruci.

Nakon otključavanja, pomoću neke od komandi spomenutih u 4 je moguće raditi sve od promjene zapisa vrijednosti glukoze do promjene vremena trajanja senzora. Svaka komanda sa sobom nosi možebitnu opasnost, od blažih poput promjene regije, koja uvjetuju vrijeme trajanja senzora, do izmjene vrijednosti glukoze koja može dovesti do ozbiljnijih posljedica.

Napad bi mogli izvršiti koristeći konfiguraciju nalik onoj na slici 11. Kod konfiguracije sa slike proxmark senzoru može slati instrukcije s do udaljednosti od 20mm. S antenom koja se može kupiti za proxmark3 ta udaljenost se može povećati na do 100mm. To omogućava da se u prolazu za manje od 1s na udaljenosti do 10cm može primjerice onesposobiti senzor.

Slika 11: Proxmark i Raspberry PI.

7 Zaključak

Kroz seminar smo se bavili pitanjem sigurnosti bežičnih medicinskih uređaja, specifično Freestlye Libre senzora. U poglavlju 2 smo opisali sam senzor, od čega se sastoji, kako mjeri vrijednosti glukoze te dali informacije o čipu kojeg koristi.
U poglavlju 3 smo pisali o uređaju kojeg smo koristili za testiranje tijekom seminara, proxmark3. Dali smo i informacije o postavljanju okruženja za rad pošto najpoznatiji *Iceman firmware* nije dostatan za izvođenje potrebnih testiranja te da ako netko bude htio replicirati testiranja može.
Poglavlje 4 se sastoji od svih mogućih napada koje smo našli za senzor te koje je moguće izvesti koristeći istu konfiguraciju kao mi.
U 5 smo elaborirali testiranja koja smo mi napravili, objasnili koje smo podatke dobili i spomenuli smo koje smo propuste napravili i na koje smo probleme naišli.
Seminar smo završili s 6 u kojem smo dali kontekst kako bi mogao napad funkcionirati da nismo naišli na prethodno spomenute probleme.

Literatura

[1] Apvrille, A., Goodspeed, T.. Security analysis of a Connected Glucose Sensor for Diabetes, https://passthesalt.ubicast.tv/protected/videos/v125f57aae7bfmvm2r6cajw3qr9nws/attachments/pts2020_talk_15_pique_curiosity_not_diabetic_fingers_technical_report.pdf

[2] NHS Scotland. What is Flash Glucose Monitoring?, https://mydiabetesmyway.scot.nhs.uk/resources/scotland-information-site/freestyle-libre-new/

[3] Cyberpunk. Proxmark 3 RDV4 Kit., https://www.cyberpunk.rs/proxmark-3-rdv4-kit

[4] Proxmark. Proxmark 3 Getting Started for Windows., https://github.com/Proxmark/proxmark/wiki/Windows