Študijsko leto 2024/2025

Ranljivosti Bluetooth naprav

Končno poročilo seminarske naloge

Urban Gajšek
Vpisna št. 63220077

Ljubljana, 20. maj 2025

Kazalo

1 Uvod

Bluetooth je brezžična komunikacijska tehnologija za prenos podatkov na kratke razdalje, ki deluje na frekvenčnem območju `2,4 GHz`. Omogoča povezovanje različnih naprav, kot so pametni telefoni, slušalke, tipkovnice, miške in drugi pametni dodatki, brez potrebe po kablih [3].

V tej nalogi sem raziskovali varnost in ranljivosti Bluetooth naprav z uporabo različnih orodij, kot so `hcitool`, `btmon`, `l2ping` in `Wireshark`. Preverjal sem dosegljivost in kakovost povezave z različnimi napravami, meril latenco, generiral dodatni promet in analiziral njegov vpliv na delovanje naprav. Prav tako sem preučil različne vrste napadov na Bluetooth ter metode zaščite pred njimi. Cilj naloge je bil bolje razumeti, kako varna (ali ranljiva) je ta tehnologija in kakšni so najboljši pristopi za njeno zaščito.

2 Dosegljivost in kakovost povezave

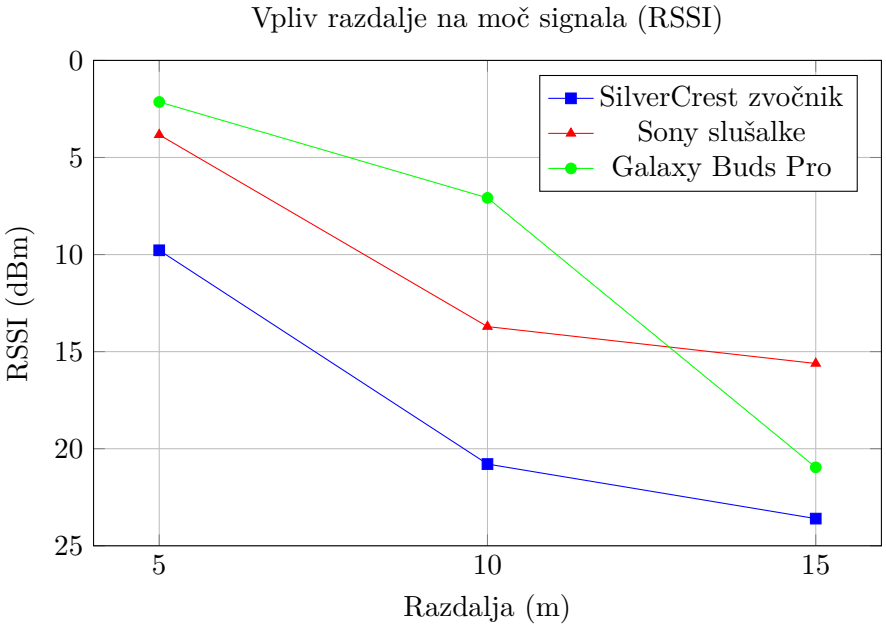
Da ugotovimo katere naprave so dosegljive, uporabimo ukaz `hcitool scan`. Ta ukaz skenira okolico in prikaže seznam imen in MAC naslovov Bluetooth naprav, ki jih najde.

Za potrebe te naloge sem uporabljal 4 različne naprave: SilverCrest bluetooh zvočnik (SBL TW6 C2), Sony Bluetooth slušalke (WH-XB910N), Galaxy Buds Pro slušalke in telefon Samsung Galaxy S22 (samo pri preučevanju napadov).

Za merjenje moči povezave sem uporabil program `btmon`, ki prikazuje podatke o povezavi v realnem času. Za lažje branje podatkov ter shranjevanja in prikazovanja grafov programa nisem zaganjal direktno, temveč sem ga ovil v svoj python program. V svojem programu sem iz izhoda `btmon` izluščil podatke o moči signala. Podane so bile RSSI vrednosti (Received Signal Strength Indicator) v enotah dBm. Na uradni strani Bluetooh je navedeno, da naj bi RSSI bile relativne vrednosti, ki naj bi bile odvisne od naprave [1]. Iz drugih virov pa sem zasledil, da naj bi bile vrednosti RSSI v dBm in da naj bi bile absolutne, ter da naj bi se gibale od okoli -20dBm (zelo dobra povezava) do -120dBm (naprava komaj zaznana) [2]. V svojih testih sem izmeril vrednosti RSSI v razponu od 0 do -30dBm. Glede na vire sem te vrednosti težko interpretiral kot absolutne vrednosti moči signala, zato sem jih obravnaval kot relativne vrednosti. Vsekakor pa so bile uporabne za določanje vpliva razdalje ter ovir na moč signala.

2.1 Vpliv razdalje na kakovost povezave

Vpliv razdalje na moč signala sem izmeril tako, da sem za vsako napravo opravil 3 eksperimente na treh različnih razdaljah (5m, 10m, 15m), nato pa sem še za vsako napravo poiskal razdaljo, na kateri se začne izgubljati povezava. Vsak eksperiment je vseboval 50 meritev iz katerih sem izluščil povprečno vrednost RSSI, nato pa sem povprečil še te tri povprečne vrednosti. Pri meritvah je bila pot od Bluetooth naprave do prenosnega računalnika, na katerega so naprave bile povezane, prosta.

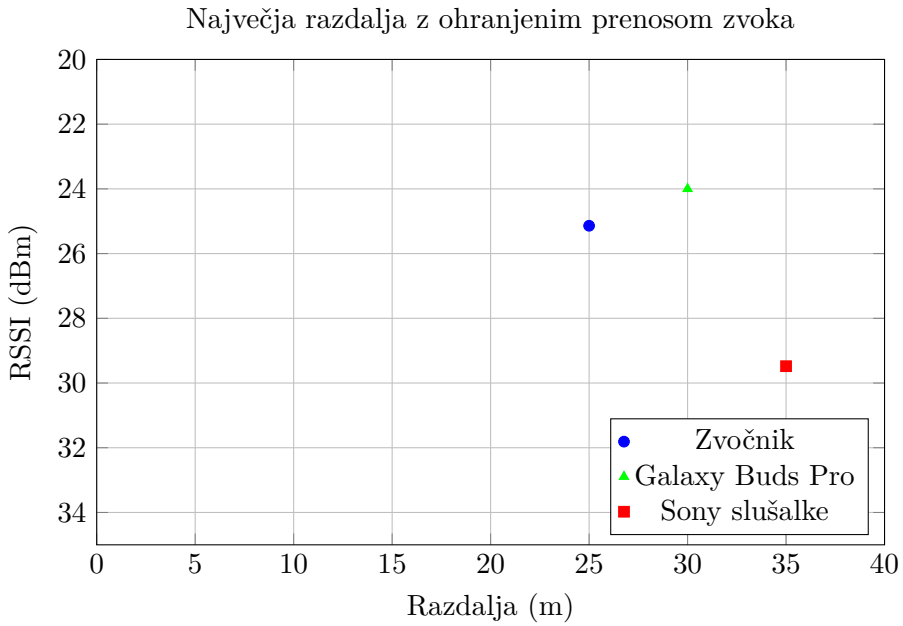


Slika 1: Meritve moči signala (RSSI) pri različnih razdaljah za tri naprave.

Kot pričakovano se moč signala z večanjem razdalje zmanjšuje. Med izvajanjem eksperimentov sem opazil, da je moč signala močno nihala. Pri Sony slušalkah sem opazil, da se je moč signala drastično spremenila, samo če sem jih zarotiral za 180 stopinj. Razlog za to je najverjetneje v tem, da je enkrat bila antena obrnjena proti računalniku, drugič pa stran od njega, na svoji poti pa je pri tem signal prepotoval čez celotno ohišje in vezje slušalk [4].

Zanimalo me je tudi, kako daleč se lahko oddaljim od naprave, da lahko še vedno nemoteno poslušam glasbo. Zaradi konsistentnosti sem na napravah predvajal šum (white noise), zato, da je bil prenos podatkov čim bolj enakomeren. Pri merjenju sem se moral oddaljevati počasi, ter med premikanjem

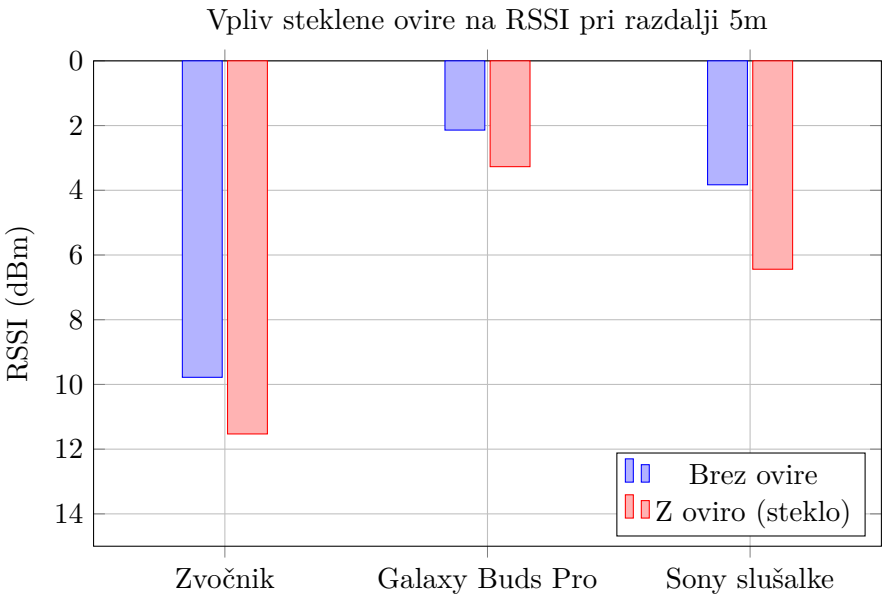
paziti, da ohranim čisto pot do prenosnika. Pri večjih ovinkih ali ovirah se je povezava hitro prekinila.



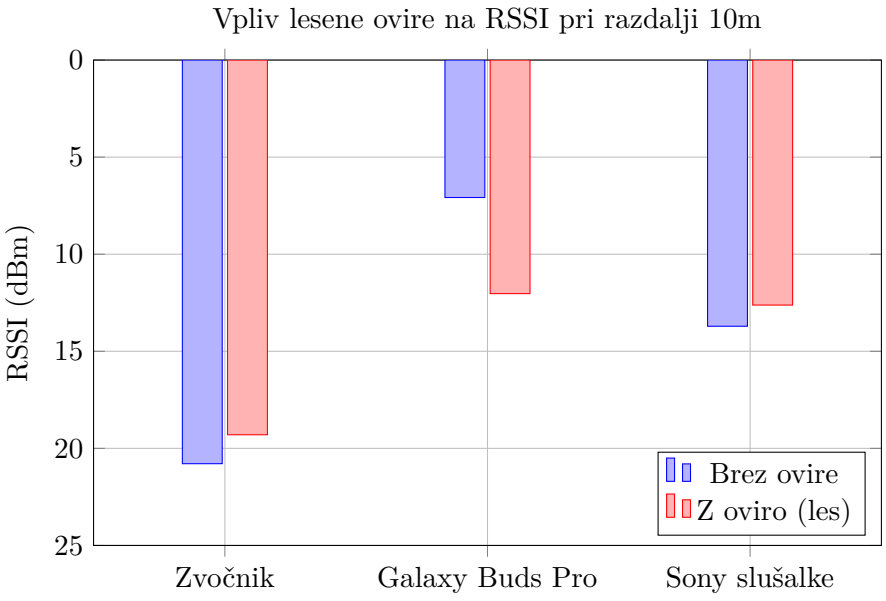
Slika 2: Dosežena največja razdalja za posamezno napravo z nemotenim predvajanjem, ter RSSI na tej razdalji.

2.2 Vpliv ovir na kakovost povezave

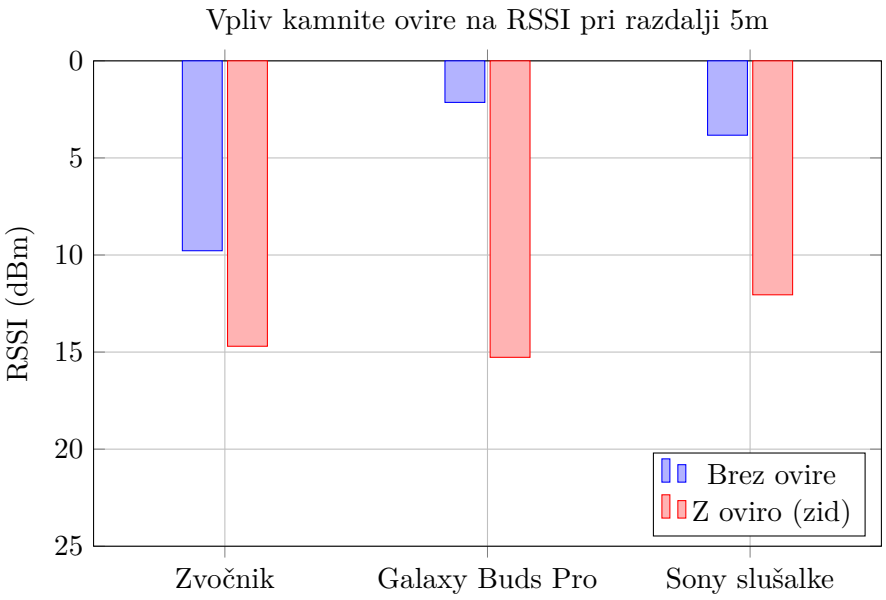
Vpliv ovir na moč signala sem izmeril tako, da sem naprave postavil na določeno razdaljo, za katero imam še izmerjeno povprečno RSSI vrednost, ob prosti poti, nato pa sem na pot postavljal razne ovire.



Slika 3: Primerjava RSSI vrednosti z in brez 1cm stekla na razdalji 5m



Slika 4: Primerjava RSSI vrednosti z in brez 2cm lesa na razdalji 10m



Slika 5: Primerjava RSSI vrednosti z in brez 30cm zidu na razdalji 5m

Iz grafov je razvidno, da tanke ovire (steklo, les) ne vplivajo močno na moč signala, medtem ko debelejše ovire (zid) povzročijo veliko izgubo moči signala.

3 Latenca in obremenitve

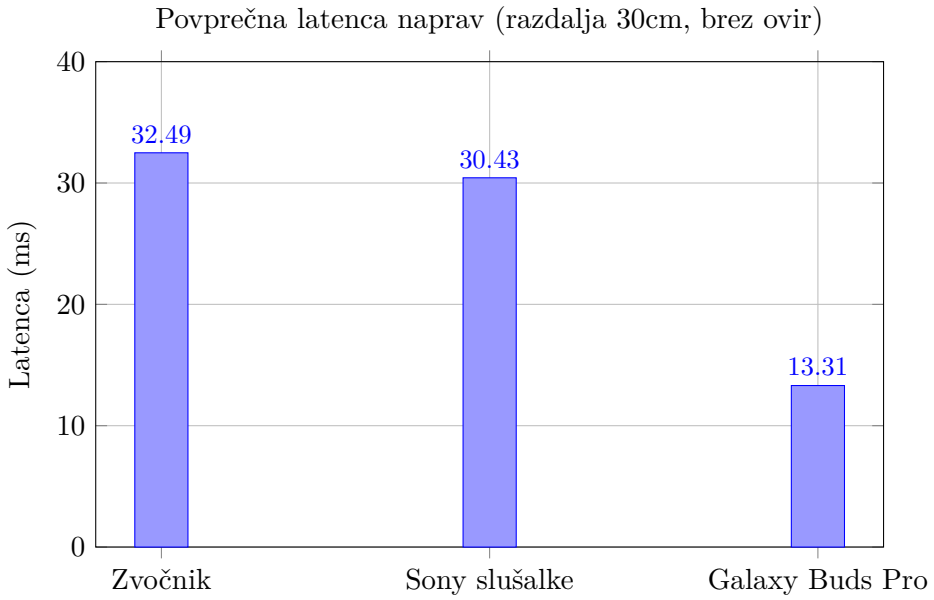
Latenco sem meril z ukazom `l2ping`, ki pošlje paket na napravo in izmeri čas, ki je potreben, da se paket vrne nazaj.

3.1 Wireshark zajem

Pri zajemu l2ping paketov z programom Wireshark lahko opazimo, da gre za protokol `L2CAP` (Logical Link Control and Adaptation Protocol) in da poteka izmenično pošiljanje paketa `Echo Request` in `Echo Response`. Vidna je tudi zakasnitev, to pa sem natančneje meril z ukazom `l2ping`.

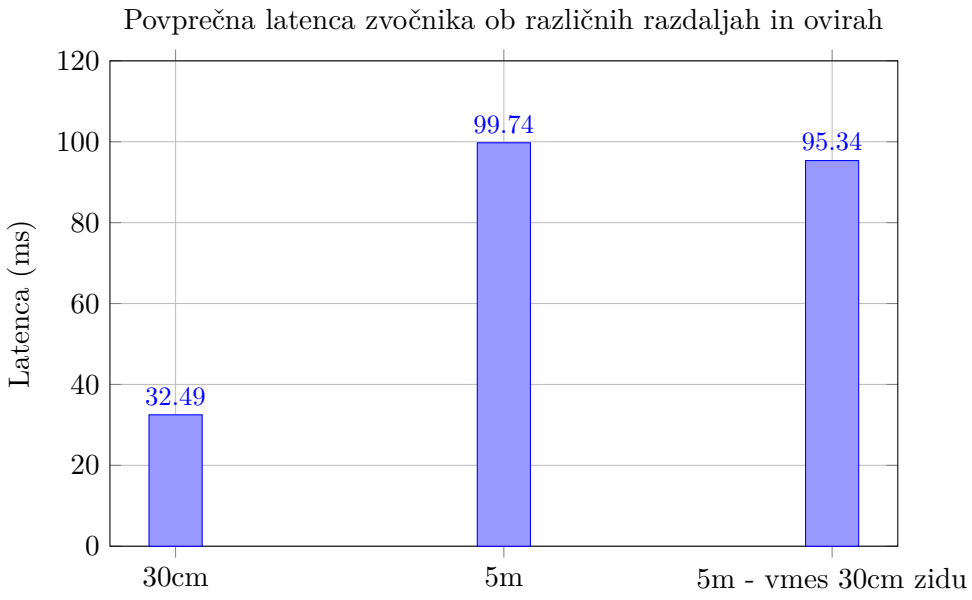
3.2 Latenca ob normalni obremenitvi

Vse meritve sem opravil na razdalji 30cm brez ovir. Za vsako napravo sem opravil 250 meritev, nato pa izračunal povprečje.



Slika 6: Povprečna latenca merjena z `l2ping` (250 paketov)

V naslednjem eksperimentu sem želel potrditi, da se latenca povečuje z oddaljenostjo, ne pa tudi z dodatnimi ovirami (dokler ni ovira tako velika, da je povezava tako slaba da se pojalja veliko število napak). Eksperiment sem izvedel samo z zvočnikom.

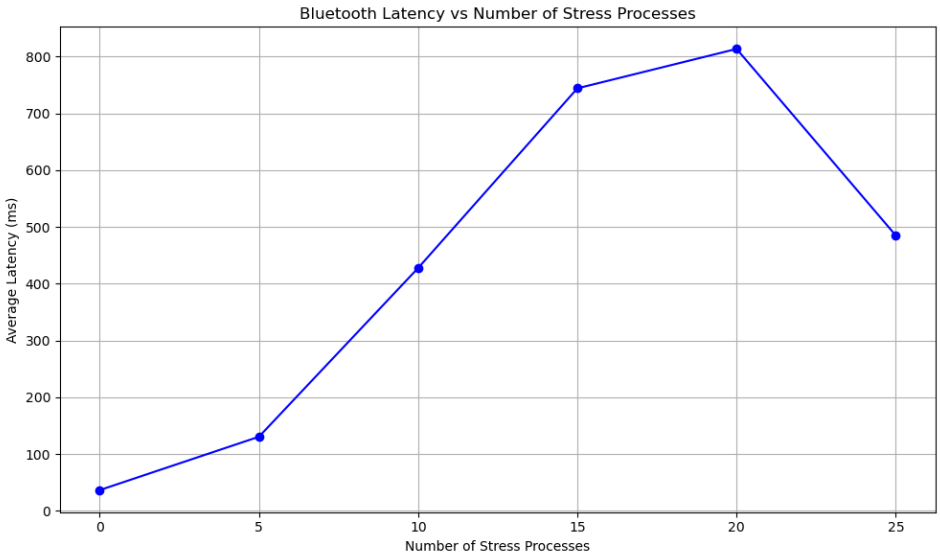


Slika 7: Povprečna latenca zvočnika merjena z `l2ping` (250 paketov)

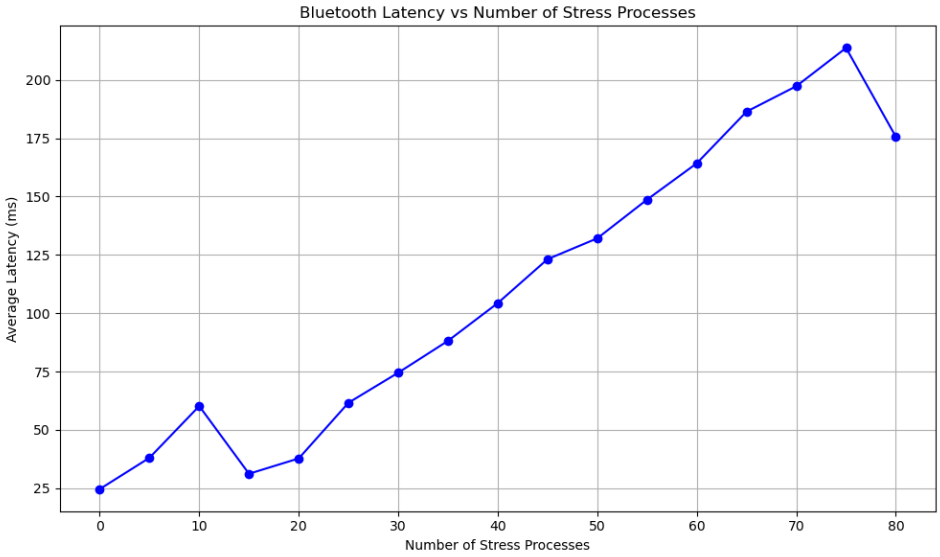
Iz grafa je razvidno, da se latenca ni bistveno spremenila z oviro, temveč le z razdaljo.

3.3 Latenca ob visoki obremenitvi

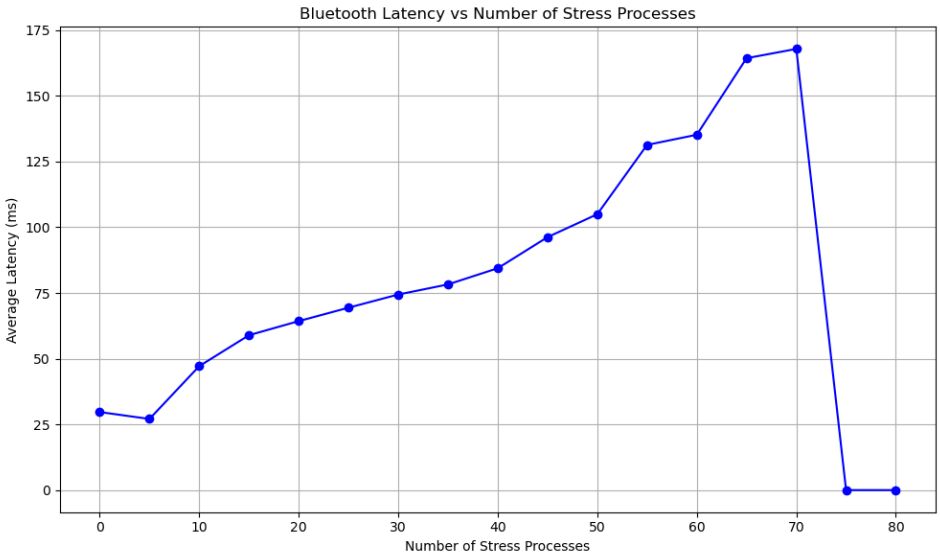
V tem eksperimentu sem želel preveriti, kako se latenca spremeni, ko napravo obremenimo z dodatnim prometom. Za to sem uporabil program `l2ing` in ga pognal z zastavico `-f` (flood). Zastavica pomeni, da program neprestano pošilja pakete z visoko frekvenco. Paralelno sem poganjal vedno več instanc programa `l2ping` in meril latenco, dokler se niso začeli izgubljati paketi, oz. dokler se naprava ni izklopila. Ob vsakem številu instanc sem opravil 50 meritev latence in izračunal povprečje.



Slika 8: Latenca zvočnika v odvisnosti od števila instanc `l2ping`



Slika 9: Latenca slušalk Galaxy Buds Pro v odvisnosti od števila instanc `l2ping`



Slika 10: Latenca Sony slušalk v odvisnosti od števila instanc `l2ping`

Latenca pričakovano narašča z večanjem števila instanc `l2ping`. Zvočnik je začel izgubljati pakete že pri 25 procesih, največja latenca pa je znašala kar 800ms. Sony slušalke so se pri 75 instancah celo izklopile.

4 Napadi na Bluetooth naprave

Moderne Bluetooth naprave (Bluetooth 6.0, 2024) so večinoma relativno varne. Seveda pa je v obtoku še vedno veliko starejših naprav, prav tako pa je še vedno obstajajo ranljivosti, ki jih je mogoče izkoristiti tudi na novejših napravah.

4.1 Pregled pogostih napadov

- **MAC Address tracking** - Ko je naprava v načinu iskanja, je njen MAC naslov viden vsem napravam v bližini. To samo po sebi ni ranljivost, vendar je velikokrat prvi korak v mnogih drugih napadih. Ker se MAC naslov naprave načeloma ne spreminja (nekatere moderne naprave ga lahko naključno spremenijo), ga lahko uporabimo kot identifikator naprave in posledično uporabnika. Trgovine bi to lahko uporabile za sledenje uporabnikom in preučevanje vzorcev nakupovalnih časov.

- **Bluejacking** - Napravi pošljemo sporočilo brez dovoljenja uporabnika. Največkrat posledice niso resne, uporabniku se lahko na primer prikaže oglasno sporočilo. Večina modernih naprav takih sporočil ne sprejema več, oz. zahtevajo, da jih uporabnik eksplicitno sprejme.
- **Bluesnarfing** - Iz naprave pridobimo zasebne podatke, kot so stiki, koledarji, sporočila in podobno. Večina modernih naprav zahteva, da uporabnik izrecno dovoli dostop do teh podatkov.
- **Bluebugging** - Pridobimo popoln nadzor nad napravo. Na modernih napravah je to brez posebnih nastavitev skoraj nemogoče.
- **Bluetooth spoofing** - MAC naslov lastne naprave spremenimo v MAC naslov druge naprave in jo s tem impersoniramo. To je lahko uporabno pri naslednjem napadu.
- **MITM** - Prestrežemo komunikacijo med dvema napravama. Povezati se moramo z obema napravama, nato pa se podatki prenašajo preko nas, mi pa jih posredujemo naprej.
- **DoS napadi** - Napravo preobremenimo z mnogo paketi, poslanimi z visoko frekvenco. Naprava se lahko izklopi ali začne počasneje delovati in izgubljati pakete. V skrajnih primerih se lahko naprava celo pregreje in uniči. Primer tega je uporaba zastavice `-f` pri ukazu `l2ping`, ki pošilja pakete z visoko frekvenco.

4.2 Demonstracija izvedljivih napadov

Najprejprej preglejmo dosegljive Bluetooth naprave:

```
$ hcitool scan
Scanning ...
        41:42:7B:CB:AC:9E       SBL TW6 C2
        44:EA:30:60:EA:58       Galaxy Buds Pro (EA58)
        F0:CD:31:60:0F:D5       Urban S22
        90:7A:58:E9:9A:BB       WH-XB910N
```

Zgoraj vidimo 4 prej omenjene naprave in njihove MAC naslove. Demonstracijo bom nadaljeval na telefonu S22, zato si bom za lažje delo shranil njegov MAC naslov:

```
$ PHONE_MAC=F0:CD:31:60:0F:D5
```

Sedaj ko imam shranjen MAC naslov, lahko poiskušam ugotoviti, kakše storitve naprava podpira. To lahko storimo s pomočjo `sdptool`:

```
$ sdptool browse $PHONE_MAC
...
Service Name: OBEX Object Push
Service RecHandle: 0x10053
Service Class ID List:
  "OBEX Object Push" (0x1105)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 12
  "OBEX" (0x0008)
Profile Descriptor List:
  "OBEX Object Push" (0x1105)
    Version: 0x0102
...
```

Med drugim je `sdptool` našel tudi storitev `OBEX Object Push`, ki omogoča pošiljanje datotek na napravo. To storitev lahko preiskusimo:

```
$ obexftp --noconn --uuid none --bluetooth $PHONE_MAC --channel 12 --put test.txt

Suppressing FBS.
Connecting..\done
Sending "test.txt".../done
Disconnecting..-done
```

S tem ukazom sem uspešno poslal datoteko `test.txt` na svoj telefon, brez da bi prej vzpostavil Bluetooth povezavo. Na telefonu sem sicer še vedno moral eksplicitno potrditi prejem datoteke, vendar pa se vsekakor lahko zgodi napaka nepozornega uporabnika, ki potrdi prejem datoteke, ki je ne želi.

Relativno enostavna je tudi izvedba `l2ping flood` napada. V tem primeru sem uporabil `l2ping` z zastavico `-f`:

```
$ sudo l2ping -s 600 -f $PHONE_MAC
Ping: F0:CD:31:60:0F:D5 from 64:79:F0:53:DD:37 (data size 600) ...
600 bytes from F0:CD:31:60:0F:D5 id 0 time 27.76ms
```

```
600 bytes from F0:CD:31:60:0F:D5 id 1 time 40.01ms
600 bytes from F0:CD:31:60:0F:D5 id 2 time 36.01ms
600 bytes from F0:CD:31:60:0F:D5 id 3 time 67.96ms
600 bytes from F0:CD:31:60:0F:D5 id 4 time 23.93ms
600 bytes from F0:CD:31:60:0F:D5 id 5 time 31.90ms
600 bytes from F0:CD:31:60:0F:D5 id 6 time 48.26ms
600 bytes from F0:CD:31:60:0F:D5 id 7 time 35.96ms
600 bytes from F0:CD:31:60:0F:D5 id 8 time 24.10ms
600 bytes from F0:CD:31:60:0F:D5 id 9 time 23.79ms
600 bytes from F0:CD:31:60:0F:D5 id 10 time 27.85ms
600 bytes from F0:CD:31:60:0F:D5 id 11 time 40.14ms
600 bytes from F0:CD:31:60:0F:D5 id 12 time 27.88ms
600 bytes from F0:CD:31:60:0F:D5 id 13 time 24.10ms
...
```

Ta ukaz sam po sebi modernim napravem ne povzroči vidnih sprememb, če pa poženemo več instanc `l2ping` pa lahko naprava začne izgubljati pakete, ali pa se celo izklopi.

5 Možni pristopi zaščite

Sodobne naprave imajo večinoma varne nastavitve, še vedno pa se je dobro zavedati potencialnih ranljivosti in se jim izogniti.

- **Onemogočite Bluetooth** - Najboljši način zaščite je, da Bluetooth izklopite, ko ga ne potrebujete. Kadar je Bluetooth izklopljen, naprava ne more biti napadena.
- **Onemogočite iskanje** - Ko naprava ni v načinu iskanja, je njen MAC naslov skrit pred drugimi napravami. Tako se izognete napadom, ki zahtevajo iskanje. Večina modernih naprav ob samem vklopu še ne preidejo v stanje iskanja, temveč je potrebna posebna akcija uporabnika.
- **Redno posodabljajte naprave** - Posodobitve vsebujejo popravke ranljivosti in izboljšave varnosti. Ko je odrita nova ranljuvost, se jo lahko s posodobitvijo programske opreme odpravi.
- **Brisanje neuporabljenih/neznanih naprav** - Naprave, ki jih ne uporabljate več, izbrišite iz seznama povezanih naprav. Veliko naprav, ki so na seznamu imajo možnost samodejne vspostavitve povezave ob vklopu Bluetootha.

- **Zavračanje sumljivih potrjevanj** - Vedno potrdimo samo zahteve ali povezave, ki smo jih sami sprožili, oz. za katere smo prepričani, da so varne.

6 Zaključek

Pri meritvah moči signala sem potrdil precej samoumevne hipoteze o vplivu razdalje na moč signala. Presenetilo me je recimo to, da so bile meritve zelo občutljive, zato sem jih moral izvesti več. Pričakoval sem tudi večji vpliv lesenih vrat na moč signala, vendar pa se je izkazalo, da je bil vpliv neopazen. Pri merjenju latence sem potrdil, da se latenca povečuje z večanjem razdalje, ne pa tudi z dodatnimi ovirami. Pri napadih me je presenetilo to, da se še vedno z lahkoto izvede `l2ping flood` napad, ki je v primeru Sony slušalk celo povzročil izklop naprave. Čeprav se varnost Bluetooth naprav veča je še vedno potrebna previdnost.

Literatura

[1] Bluetooth. Proximity and rssi. https://www.bluetooth.com/blog/proximity-and-rssi/.

[2] bluetoothle. Rssi. https://bluetoothle.wiki/rssi.

[3] Nathan J. Muller. Networking a to z. https://books.google.si/books?id=0qv4KbasX7wC&q=bluetooth&pg=PA45&redir_esc=y#v=snippet&q=bluetooth&f=false.

[4] Sony. Sony wh-xb910n wireless noise cancelling headphones. https://helpguide.sony.net/mdr/whxb910n/v1/en/contents/TP1000442871.html.