

BEZBEDNOST BLUETOOTH KOMUNIKACIJA

ppuk. mr Gorazd Zavodnik, dipl. inž., Vojna Akademija Vojske Srbije, Beograd,
gorazd.zavodnik@gmail.com, gorazd.zavodnik@yahoo.com

Apstrakt: *Bluetooth tehnologija i standard predstavljaju najjednostavniji izbor za povezivanje uređaja malg dometa (10 do 100m). Bluetooth uređaji koriste ISM frekventni opseg i formiraju mreže koje mogu imati do 8 uređaja, od kojih je jedan glavni (master) a ostali su klijenti (slave). Prema specifikaciji Bluetooth-a postoje tri bezbednosna režima: nebezbedan, bezbedan na nivou usluga i bezbedan na nivou veze. Kao i ostali uređaji koji ostvaruju međusobne veze, i Bluetooth uređaji mogu biti meta raznih napada. Napadi mogu biti bezazleni u tehničkom ismislu, a mogu imati i ozbiljnije posledice po pitanju privatnosti, integriteta podataka u mobilnom telefonu i slično. U radu su opisani neki od stvarnih, kao i eksperimentalnih napada i njihove moguće posledice.*

Ključne reči: *Bluetooth, bezbednost, napad, protivmere*

1. Uvod

Bežična *Bluetooth* tehnologija je najjednostavniji izbor za komunikacije između uređaja malog dometa i predstavlja globalno raspoloživ standard. Trenutno je na raspolaganju četvrta verzija specifikacije, uz nastavak razvoja dosadašnjih pogodnosti (mala snaga, niski troškovi, bezbednost, robusnost, lakoća upotrebe i umrežavanje u trenutku potrebe). Danas se isporučuje preko pet miliona jedinica nedeljno, dok je krajem 2005. godine bilo instalirano oko 500 miliona jedinica. *Bluetooth* tehnologija ne zahteva fiksnu infrastrukturu i jednostavna je za instaliranje i podešavanje. Uređaj se bez problema povezuje drugim Bluetooth uređajima koji imaju iste profile. Potvrda PIN kodom je jednostavna kao i prilikom prijavljivanja na bankomatu.

2. Bežični LAN

2.1. Bluetooth tehnologija

Bluetooth je prvobitno bio zamišljen kao zamena za kablove u bežičnim komunikacijama, međutim planiran je razvoj širokog spektra korisničkih uređaja i poboljšanje bežičnog povezivanja. Danas je Bluetooth standardizovan unutar IEEE 802.11 PAN radne grupe formirane početkom 1999. godine. Namenjen je za funkcionisanje u nelicenčnom ISM području, koje je uz manje varijacije na nekim mestima, dostupno na većini mesta u svetu. Uređaji će automatski detektovati i locirati druge uređaje, ali je za njihovo povezivanje potrebna akcija korisnika. Uspostavljena mreža ima privremenu i slučajnu topologiju.

Jedna od osobina Bluetooth mreža je odnos upravljač – klijent (master – slave). Na taj način se međusobno može povezati do 8 uređaja u tzv. pikomrežu (piconet), sa jednim uređajem koji je "upravljač", dok su ostali povezani kao

"klijenti". Glavni uređaj kontroliše i podešava mrežu. Iako samo jedan uređaj može da bude glavni u jednoj pikomreži, klijent u jednoj mreži može biti upravni u nekoj drugoj mreži, čime se formira lanac mreža i omogućava povezivanje na veće udaljenosti.

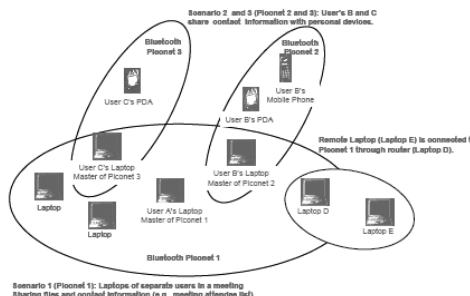
Tabela 1. Frekventni opsezi u nekim zemljama

Zemlja	Frekventni opseg	RF kanali	
Evropa i SAD	2400 – 2483,5 MHz	$f = 2402 + k$ MHz	$k = 0, \dots, 78$
Japan	2471 – 2497 MHz	$f = 2473 + k$ MHz	$k = 0, \dots, 22$
Španija	2445 – 2475 MHz	$f = 2449 + k$ MHz	$k = 0, \dots, 22$
Francuska	2446,5 – 2483,5 MHz	$f = 2454 + k$ MHz	$k = 0, \dots, 22$

U Bluetooth specifikaciji osim normalnog aktivnog režima postoje i razni osnovni režimi koji omogućavaju uštedu energije, omogućavanjem da radio čipovi na robovi ma uđu u režim parkiranja (park), osluškivanja (sniff) ili zadržavanja (hold) Bluetooth konekcije (ali ne i celog uređaja). Kada uređaj nije u vezi, nalazi se u stanju pripravnosti (standby).

Više pikomreža može formirati scatternet (slika 1). Upravni uređaj u jednoj pikomreži može biti klijent u drugoj pikomreži, a uređaji mogu istovremeno biti klijenti u više pikomreža. Za prebacivanje između pikomreža koristi se vremensko multipleksiranje. Topologija scatternetu obezbeđuje fleksibilan metod kojim uređaji održavaju višestruke veze.

Slika 1. Tipična Bluetooth mreža – raspršena mreža (scatternet)



Bluetooth obezbeđuje tri različite klase upravljanja snagom. Uređaji prve klase (najveće snage) imaju 100 mW i domet do 100 m. Uređaji druge klase imaju snagu 2.5 mW i domet do 10 m. Uređaji treće klase (najmanje snage) imaju 1 mW i domet od 10 cm do 10 m.

2.2. Bezbednost Bluetooth-a

Prema specifikaciji Bluetooth raspolaže sa tri bezbednosna režima:

- Bezbednosni režim 1 – nebezbedan režim,
- Bezbednosni režim 2 – bezbednost na nivou servisa,
- Bezbednosni režim 3 – bezbednost na nivou veze.

Pre primene Bluetooth tehnologije potrebno je razmotriti bezbednosne pretnje, kao i ranjivosti uređaja koji će učestvovati u Bluetooth mrežama. Posebnu pažnju treba obratiti na tajnost, integritet podataka i raspoloživost mreže. Neželjenim bezbednosnim propustima će doprineti i korisnici uređaja koji su manje svesni opasnosti nego administratori bezbednosti, a češće će upravljati uređajima.

Osnovne bezbednosne pretnje možemo podeliti na napa de na tajnost, integritet i raspoloživost (dostupnost). Protivmere koje pomažu kod obezbeđivanja Bluetooth mreža su: upravne, operacione i tehničke.

3. MOGUĆI NAPADI NA BLUETOOTH

• Bluejacking

Bluejacking je slanje lažnih poruka pomoću Bluetootha uređajima koji su opremljeni Bluetooth–om. Poreklo naziva nije najpouzdanije. Preovlađuje uverenje da je nastao od reči Bluetooth i hijacking (autostopiranje). Napadač međutim nikoga ne stopira nego samo koristi osobine uređaja koje imaju pošiljaoc i primalac. Obe strane zadržavaju apsolutnu kontrolu nad svojim uređajima, dok napadač ne može preuzeti telefon ili ukrasti lične informacije.

• Praćenje (Wardriving)

Praćenje je pronalaženje lokacija na kojima se nalaze korisnici uređaja sa Bluetooth–om. Pošto svaki uređaj slobodno emituje svoju jedinstvenu 48–bitnu adresu, omogućava praćenje kretanja. Zaštita uređaja od lociranja postiže se anonimnim režimom rada, u kojem uređaji redovno ažuriraju svoju adresu slučajnim izborom nove. Mogući oblici lociranja su ispitivanje, praćenje saobraćaja, paging i frekvencijsko skakanje.

• Neovlašćen pristup (Bluesnarfing)

Bluesnarfing je neovlašćen pristup informacijama u bežičnom uređaju pomoću Bluetooth konekcije. Omogućen je pristup kalendaru, imeniku, e–pošti i tekstualnim porukama. Ranije je bilo i slučaja pozivanja značajnih brojeva bez znanja korisnika. Bilo koji uređaj sa aktiviranom Bluetooth konekcijom podešenom na "dostupan" (može da je otkrije drugi Bluetooth uređaj koji se nalazi u blizini) može biti meta napada. Prelaskom u režim "skriven" bezbednost je povećana, mada postoje načini da se napadnu i skriveni uređaji.

• BlueBug

BlueBug je naziv za propust u bezbednosti Bluetootha na mobilnom telefonu. Zloupotreba tog propusta omogućava neovlašćen pristup podacima u telefonu. U idealnim uslovima napad traje nekoliko sekundi, zavisno od postupaka u toku napada. Zbog ograničene prenosne snage bluetooth radia klase 2, distanca između napadača i napadnutog ne sme da prelazi 10 – 15 metara. U cilju povećanja dometa može se koristiti usmerena antena. Neki primeri su:

- iniciranje telefonskog poziva,
- slanje SMS na bilo koji broj,
- čitanje SMS sa telefona,
- čitanje i pisanje po telefonskom imeniku,
- podešavanje preusmeravanja poziva,
- povezivanje na Internet,
- prisilna upotreba određenog provajdera, ...

• Napad grubom silom

Radi se o brutalnom napadu na MAC adresu uređaja koji se nalazi u režimu mogućeg otkrivanja, pa čak i u skrivenom režimu. Neki proizvođači tvrde da je za tako nešto potrebno nerazumno mnogo vremena (npr. 11 sati). Međutim @stake's RedFang verzijom koja radi višekanalno i može istovremeno uposliti do 8 USB

Bluetooth uređaja, vreme se može skratiti na oko 90 minuta. Nakon otkrivanja sdrese moguće je izvršiti Bluesnarf napad jer je korisnik ubeđen da je bezbedan ako je uređaj u skrivenom režimu.

- **DoS napad (blokiranje usluga)**

U slučaju neuspešne autentikacije Bluetooth uređaja mora da prođe određeno vreme pre novog pokušaja verifikatora da uputi zahtev za autentikaciju istom uređaju i da uređaj odgovori na zahtev. Nakon svake sledeće neuspešne autentikacije interval čekanja se eksponencijalno produžava do neke maksimalne vrednosti. Napadač sprečava ili zabranjuje normalnu upotrebu ili upravljanje komunikacionim resursima. Do degradacije sistema dolazi zbog zauzetosti opsluživanjem zlonamernih zahteva za povezivanje.

- **Napad sa presretanjem (Man in the Middle)**

Ovaj napad predstavlja dodatnu pretnju jednostavnim "glupim" uređajima koji se oslanjaju na jedinični ključ. Presretač (uređaj C) dobavlja bezbednosni ključ za šifrovanje kojeg mrežni uređaj (A) koristi za kontrolu saobraćaja sa nekim drugim mrežnim uređajem (B). Sve što je za to potrebno je da uređaj A odvojeno podeli svoj jedinični ključ sa uređajima B i C. Razlozi za komunikaciju uređaja A i B i uređaja A i C mogu biti potpuno nepovezani i sa različitim nivoima poverenja. U svakom slučaju, nakon što uređaj C sazna jedinični ključ, može pomoću lažne adrese uređaja izračunati ključ za šifrovanje i nadgledati saobraćaj između uređaja A i B bez njihovog znanja.

- **Napad na privatnost**

Postoje razne komponente privatnosti. Najopštija podela obuhvata: anonimnost, pseudonim, nepovezivanje i neposmatranje. *Anonimnost* podrazumeva upotrebu resursa bez otkrivanja identiteta. *Pseudonim* daje korisniku pravo upotrebe, bez otkrivanja identiteta, uz zamenski naziv. *Nepovezivanje* obezbeđuje da korisnik može koristiti veći broj resursa ili usluga bez mogućnosti da ostali oüče vezu između tih korišćenja. Namena toga je prikrivanje povezanosti akcija istog korisnika. *Neposmatranje* obezbeđuje da može korisnik koristiti resurse, pri čemu treća strana to ne može da uoči. Na primer da se prilikom emitovanja prikrije ko je u stvari pošiljalac a ko primalac informacija. Relativno nova je tzv. *privatnost lokacije*. To je mogućnost sprečavanja otkrivanja trenutne ili neke ranije lokacije.

- **Udaljeni Snarf**

Udaljeni Snarf je eksperiment koji je izveden 4. avgusta 2004. godine ujutro u Kaliforniji (Santa Monica Pier). Izveli su ga John Hering, James Burgess, Kevin Mahaffey, Mike Outmesguine i Martin Herfurt u saradnji sa TV stanicom G4TechTV. Mike (kameran TV ekipe) i Martin su otišli na uzvišenje udaljeno 1,78 km od parkinga na kojem su ostali John, James i Kevin koji su pripremali opremu potrebnu za eksperiment. U samom eksperimentu je ekipa napadača usmerila antenu ka lokaciji. Nakon manjih problema oko pronalaženja telefonskog uređaja na velikoj udaljenosti desilo se nešto neverovatno. Na ekranu telefona Nokia, koji je Mike držao u ruci, prikazale su se stvari tipične za BlueBug napad. Najpre tekst "Connected to ..." i nakon toga mali simbol slušalica. Time je pokazano da se uređaju sa Bluetooth uređajem klase 2 (domet oko 10 m) može pristupiti sa oko 170 puta veće udaljenosti od deklarisanе.

Slika 2. Članovi ekipe



Slika 3. Martin i Mike na uzvišenju, strelica pokazuje lokaciju ostatka ekipe (napadača)



Ovakav napad objašnjava kolikom riziku mogu biti izloženi vlasnici ranjivih telefona.

U eksperimentu je korišćena sledeća oprema:

- Laptop Dell sa operativnim sistemom Slackware Linux 9.1 i BlueZ biblioteke i alati verzije 2.9;
- Modifikovani USB Bluetooth adapter marke Linksys sa spoljnim antenskim konektorom;
- Snažna (19dBi) antena (najbolje ako je tipa Short Backfire) i
- Nemodifikovani telefon Nokia 6310i.

• Blooover

Blooover je alat namenjen za izvršavanje na mobilnim telefonima koji podržavaju J2ME. Zamišljen je kao alat za nadzor i proveru da li je telefon ranjiv. Nakon uspeha alata Blooover i oko 150000 downloada u 2005. godini napravljen je alat Blooover II koji osim napada BlueBug omogućava i neke druge napade.

• BlueDump

Posledica BlueDump-a je da Bluetooth uređaj odbaci upisani ključ linka i time stvara mogućnost 'njuškanja' u toku razmene ključeva. Prvi koji je pisao o napadima na ključeve linka i PIN-ove je bio Ollie Whitehouse, koji je opisao metod kojim se mogu dobiti PIN i ključevi linka ukoliko se odgovarajućim alatom (Bluetooth sniffer) može pratiti tok uparivanja.

• BlueChop

BlueChop je napad koji narušava uspostavljenu Bluetooth pikomrežu uređajem koji nije učesnik u pikomreži. Preduslov za takav napad je da upravni uređaj pikomreže podržava višestruko povezivanje. U toku napada uređaj koji nije učesnik u pikomreži, na slučajan način bira jednog od klijentskih uređaja iz

pikomreže, lažno se predstavlja i kontaktira upravni uređaj. To dovodi zbunjivanja unutrašnjeg stanja upravnog uređaja i narušava pikomrežu.

- **Napad kroz uparivanje, otkrivanje PIN-a bez uspostave veze**

Bluetooth specifikacije je osetljiva na pasivne i aktivne napade u toku procedure uparivanja. Napad uspeva samo ako je napadač prisutan prilikom uparivanja, koje se između dva uređaja dešava samo jednom. Ukoliko se uparivanje vrši na javnom mestu, npr. prilikom povezivanja sa pristupnom tačkom ili štampačem, to može biti ozbiljna pretnja, pošto napadač može prisluškivati prenosu podataka u toku uparivanja.

- **Otkrivanje PIN-a u toku veze**

Napad je moguć kada uređaj koristi fiksni PIN, isti za svaki uređaj sa kojim se povezuje. Napadač može u toku napada nekoliko puta promeniti BD_ADDR i testirati različite PIN kodove. Menjanjem Bluetooth adrese napadač izbegava produžavanje pauze između neuspešnih pokušaja uparivanja.

- **Napadi sa ponavljanjem poruka**

Napadač može snimiti Bluetooth saobraćaj na svih 79 frekvencija i na neki način otkriti sekvencu frekvencijskog skakanja, da bi ponovio prenos. Iako može napad zahtevati posebnu opremu, moguć je pošto Bluetooth uređaji ne znaju da li se radi o staroj ili novoj poruci.

- **Car Whisperer**

Projektom CarWhisperer pokušava da se ukaže proizvođačima Bluetooth uređaja (bez tastature i ekrana) za kola, na moguće bezbednosne pretnje u slučaju upotrebe standardnih lozinki. Carwhisperer se povezuje sa uređajem kojeg je otkrio skener. Nakon jednom uspešno uspostavljene konekcije šalju se audio signali slušalici i snimaju se audio signali od slušalice. To omogućava napadaču da ubaci audio podatke u vozilo. Napadači mogu i prisluškivati razgovore između ljudi koji sede u kolima. U idealnom slučaju, koristi se sa friziranim priključkom i usmerenom antenom koja prilično povećava domet.

Slika 4. Traženje uređaja u vozilima



4. Zaključak

Bluetooth tehnologija osim olakšanog povezivanja uređaja malog dometa sa sobom nosi i određene bezbednosne pretnje. U radu su prikazani najčešći tipovi praktičnih i eksperimentalnih napada. Najjednostavnija protivmera je da korisnici

vode računa o okruženju u kojem uspostavljaju veze. Dopunama standarda i definisanjem i primenom novih bezbednosnih mehanizama, postupaka i šifarskih sistema pretnje se mogu značajno umanjiti, ali se ne mogu ukloniti.

5. Literatura

- [1] Bluetooth Technology (www.bluetooth.com/bluetooth/learn)
- [2] Bluetooth Tutorial (www.palowireless.com/bluetooth)
- [3] Korak Dasgupta: Bluetooth Protocol and Security Architecture Review
- [4] Sil Janssens: Attacking Bluetooth Devices (2005)
- [5] Sil Janssens: Bluetooth Tools (2005)
- [6] Sil Janssens: Internship Report – Bluetooth Security (2004)
- [7] Sil Janssens: Preliminary Study – Bluetooth Security (2005)
- [8] Trifinite Group (www.trifinite.org)

SECURITY OF BLUETOOTH COMMUNICATIONS

Apstract: *Bluetooth technology and standard represent the easiest way to connect devices with short range (10 to 100m). Bluetooth uses an ISM frequency range, forming networks with at most 8 devices of which is one master and the others are slaves. According to specificatin there are 3 security modes: unsecure, secure on service level and secure on link level. As all others devices which connect to others, Bluetooth devices can be targets of various attacks. The attacks can be meaningless in technical sense, but they can also have consequences to privacy and data integrity. In this paper are described various attacks, real and experimental, and their possible consequences.*

Keywords: *Bluetooth, security, attack, countermeasures*