CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Ranjivosti Bluetooth tehnologije

NCERT-PUBDOC-2009-11-281

Nacionalni CERT

u suradnji s

LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem Nacionalni CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom Nacionalnog CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

Nacionalni CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Bežične tehnologije koriste se za prijenos podataka na veće ili manje udaljenosti različitim brzinama uz različitu kvalitetu. Jedna od tehnologija koja spada u ovu skupinu je i Bluetooth - standard koji definira prijenos raznih vrsta podataka na relativno malim udaljenostima (do 100 m). Radi se o standardu kojeg razvija i definira organizacija Bluetooth SIG (eng. Special Interest Group), a prvi put se pojavio 1998. godine. U specifikaciji standarda određeni su parametri povezivanja, kao i korišteni pojas frekvencija, modulacija i dr. Budući da omogućuje povezivanje malih uređaja (mobitela i sl.) u privremenu mrežu (koji tada imaju mogućnost međusobne komunikacije), tehnologija je doživjela veliki uspjeh i brzo postigla iznimnu popularnost.

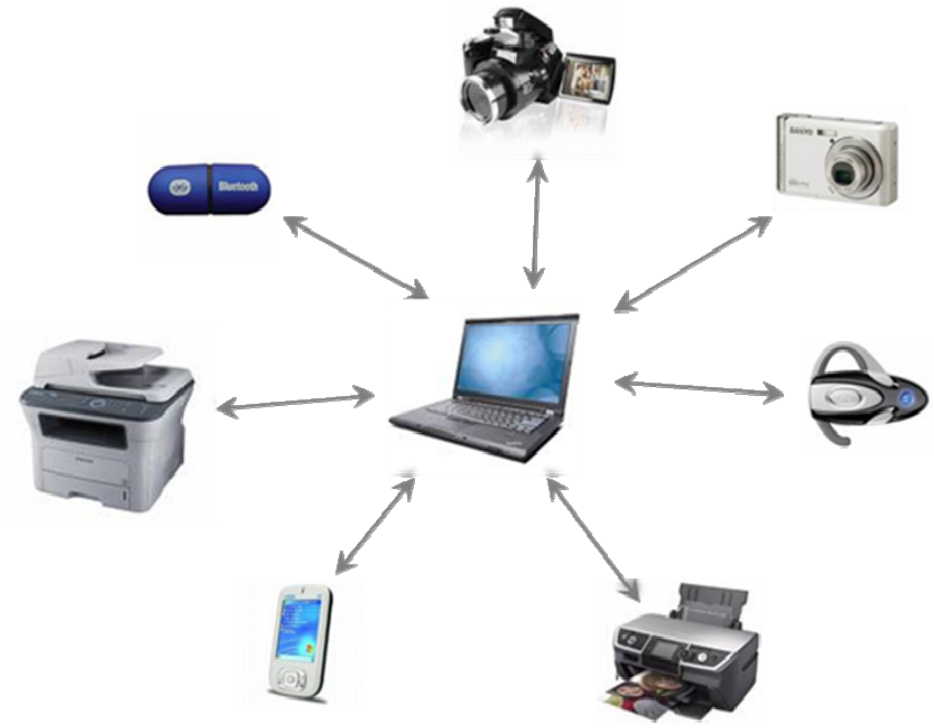
Od prve pojave ove tehnologije otkrivene su razne ranjivosti u definiranoj specifikaciji. Neke od njih javljaju se u postupku autentikacije i kriptiranja ili su posljedica nepravilnog rukovanja parametrima za ostvarivanje veza. Zlonamjernim korisnicima ovakve ranjivosti omogućuju izvođenje raznih napada koji omogućuju pregled korisničkih podataka, ostvarivanje veza s drugim uređajima i sl. Neki od poznatijih napada su *Blujacking* (koji predstavlja jednostavno lažne slanje poruke na drugi uređaj) i *Bluebugging* (koji uključuje potpuno preuzimanje nadzora nad uređajem).

U nastavku dokumenta dan je opis Bluetooth tehnologije i postojećih specifikacija. Zatim je dan uvod u sigurnost tehnologije i pregled poznatijih napada. Na kraju su navedene mjere zaštite uz osvrt na budući razvoj spomenutog standarda.

2. Bluetooth

Bluetooth je bežični protokol za razmjenu podataka na kratkim udaljenostima između fiksnih i/ili mobilnih uređaja. Služi za spajanje nekoliko uređaja uz rješavanje problema sinkronizacije, a primjer jednog povezivanja dan je na slici 1. Navedena slika prikazuje „*piconet*“ mrežu gdje se uređaji (najviše 8 uređaja) povezuju tako da jedan od njih predstavlja glavni uređaj (master) te provodi sinkronizaciju ostalih. U danom primjenu glavni uređaj je osobno računalo., dok ostali predstavljaju „robove“ (eng. slaves). Temelji se na izgradnji PAN (eng. personal area network) mreže koja se koristi za komunikaciju osobnih uređaja na malim udaljenostima (npr. unutar nekoliko metara).

Originalno je razvijen kao alternativa RS-232 (eng. Recommended Standard 232) podatkovnim kablovima. Bluetooth koristi radio tehnologiju pod nazivom „prošireni spektar s frekvencijskim skakanjem“, koja definira podjelu podatka na manje dijelove te slanje na jedu od 79 definiranih frekvencija. U osnovnom načinu rada koristi se GFSK (eng. Gaussian frequency-shift keying) modulacija te se može postići brzina prijenosa do 1 Mbps. Bluetooth pruža način za povezivanje i razmjenu informacija između uređaja kao što su mobilni telefoni, prijenosna računala, fiksni telefoni, osobna računala, pisači, GPS (eng. Global Positioning System) uređaji, digitalna kamere i dr. Prijenos se odvija preko sigurnog, globalno nelicenciranog (njegova uporaba se ne naplaćuje) ISM (eng. Industrial, Scientific and Medical) pojasa na 2.4 GHz. Specifikaciju je razvila i licencirala udruga Bluetooth SIG (eng. Special Interest Group) koju čine brojne organizacije iz područja telekomunikacija, računarstva, mrežnih usluga i elektronike (značajniji članovi: „Ericsson Technology Licensing“, „Lenovo“, „Intel“, „Microsoft“, „Motorola“, „Nokia“, „Toshiba“ i dr.).



Slika 1 Povezivanje uređaja Bluetooth vezama

2.1. Uporaba

Bluetooth standard i komunikacijski protokol je primarno dizajniran za uporabu na uređajima niske cijene i male potrošnje energije kako bi im omogućio međusobnu komunikaciju. Uređaji se dijele u tri klase prema potrošnji energije i najvećoj udaljenosti na način prikazan u tablici 1.

Klasa	Najveća energija / mW (dBm)	Približna udaljenost / m	Primjer
1	100 (20)	~ 100	Bluetooth USB, Modem i sl.
2	2,5 (4)	~ 22	Bluetooth USB, tastatura, miš i sl.
3	1 (0)	~ 6	Bluetooth adapter, slušalice i sl.

Tablica 1 Klase Bluetooth uređaja

Najčešće se koristi za sljedeće namjene:

- bežična komunikacija između mobilnih uređaja i slušalica,
- bežična mreža između osobnih računala u uvjetima kada je dostupna mala širina pojasa,
- bežična komunikacija s ulaznim i izlaznim uređajima osobnih računala (miš, tipkovnica, printer),
- prijenos datoteka i podataka između uređaja OBEX (eng. OBject EXchange) protokolom,
- zamjena za tradicionalne žičane komunikacije u ispitnoj opremi, GPS uređajima, medicinskoj opremi, *BarCode* skenerima i sl.,
- nadzor kod sustava koji koriste IR (eng. Infrared radiation) tehnologije,
- programi koje ne zahtijevaju veliku širinu prijenosnog pojasa te nisu ovisni o kabelskim vezama,
- bežični most između industrijskih Ethernet mreža,
- bežični nadzor igraćih konzola i
- pristup Internetu na osobnom računalu uporabom mobilnog uređaja kao modema.

2.2. Specifikacije

Bluetooth specifikaciju razvili su 1994. godine Jaap Haarsten i Sven Mattisson, zaposlenici firme „Ericsson Mobile Platforms“ u Švedskoj. Udruga Bluetooth SIG, koju su osnovale tvrtke Ericsson, IBM, Intel, Toshiba i Nokia, obradila je te javno objavila specifikaciju 20. ožujka 1998. godine. Danas spomenuta udruga uključuje preko 11.000 članica diljem svijeta.

Prva inačica protokola bila je **Bluetooth 1.0,** koja je ubrzo proširena određenim nadopunama na inačicu **Bluetooth 1.0B**. Zbog brojnih problema u tim specifikacijama, proizvođači su imali problema s omogućivanjem međusobne komunikacije njihovih uređaja. Također, specifikacije su uključivale prijenos BD_ADDR (eng. Bluetooth hardware device address) adresa pa nije bilo moguće osigurati anonimnost.

Mnoge pogreške pronađene u Bluetooth specifikaciji ispravljene su u novoj inačici pod nazivom **Bluetooth 1.1.**, koja je dobila oznaku IEEE (eng. Institute of Electrical and Electronics Engineers) standarda 802.15.1-2002. Između ostalog, dodana je podrška za nekriptirane kanale te uvedeno mjerenje RSSI (eng. Received Signal Strength Indicator) vrijednosti, tj. snage u prijamnom radio kanalu.

Sljedeća inačica bila je **Bluetooth 1.2,** koja je u potpunosti sukladna s prethodnom inačicom uz sljedeća poboljšanja:

- brže povezivanje i otkrivanje uređaja,
- veća brzina prijenosa podataka,
- bolja kvaliteta govora preko audio kanala,
- uvedena provjera toka podataka.

Opisana inačica poznata je kao IEEE standard 802.15.1-2005.

Inačica **Bluetooth 2.0** objavljena je 10. studenog 2004. godine, a osnovna razlika u odnosu na prethodnu inačicu je uvođenje bržeg prijenosa podataka. To je postignuto korištenjem tehnologije EDR (eng. Enhanced Data Rate), čija je nominalna brzina oko 3 Mbps. Prednosti koje donosi spomenuta tehnologija su:

- tri puta veća brzina prijenosa podataka,
- smanjena složenost korištenja više simultanih veza i
- smanjena uporaba energije.

Organizacija Bluetooth SIG objavila je specifikaciju s opcionalnom mogućnošću uporabe EDR tehnologije.

Dana 26. srpnja 2007. godine, udruga Bluetooth SIG objavila je novu specifikaciju - **Bluetooth 2.1** sa sljedećim obilježjima:

- EIR (eng. Extended Inquiry Response) – pružanje više informacija (ime uređaja, lista podržanih usluga i sl.) tijekom procedure traženja uređaja.
- Smanjena potrošnja energije – posebno kada se uređaj nalazi u „*sniff*“ načinu rada.
- EPR (eng. Encryption Pause/Resume) – omogućuje jednostavniju razmjenu ključeva za kriptiranje.
- SSP (eng. Secure Simple Pairing) – poboljšanje spajanja Bluetooth uređaja uz veću sigurnost.
- NFC (eng. Near Field Communication) – automatsko stvaranje sigurnih Bluetooth veza.
- NAF-PBF (eng. Non-Automatically-Flushable Packet Boundary Flag) – mogućnost sinkronog i asinkronog prijenosa preko iste logičke veze.

Dodatna poboljšanja donosi specifikacija **Bluetooth 3.0**, koja je objavljena 21. travnja 2009. godine. Osnovne novosti koje uvodi ova inačica uključuju:

- AMP (eng. Alternate MAC/PHY) – omogućuje uporabu fizičkog ili MAC sloja za prijenos podataka o Bluetooth profilu.
- UCD (eng. Unicast Connectionless Data) – omogućavanje slanja podataka bez uspostavljanja eksplicitnih kanala.
- otkrivanje veličine ključa za kriptiranje – uvođenje standardne naredbe za upit o duljini ključa za kriptiranje na kriptiranoj vezi.
- uveden dodatni nadzor energije – uvedena bolja provjera energije u skladu s uporabom uređaja.

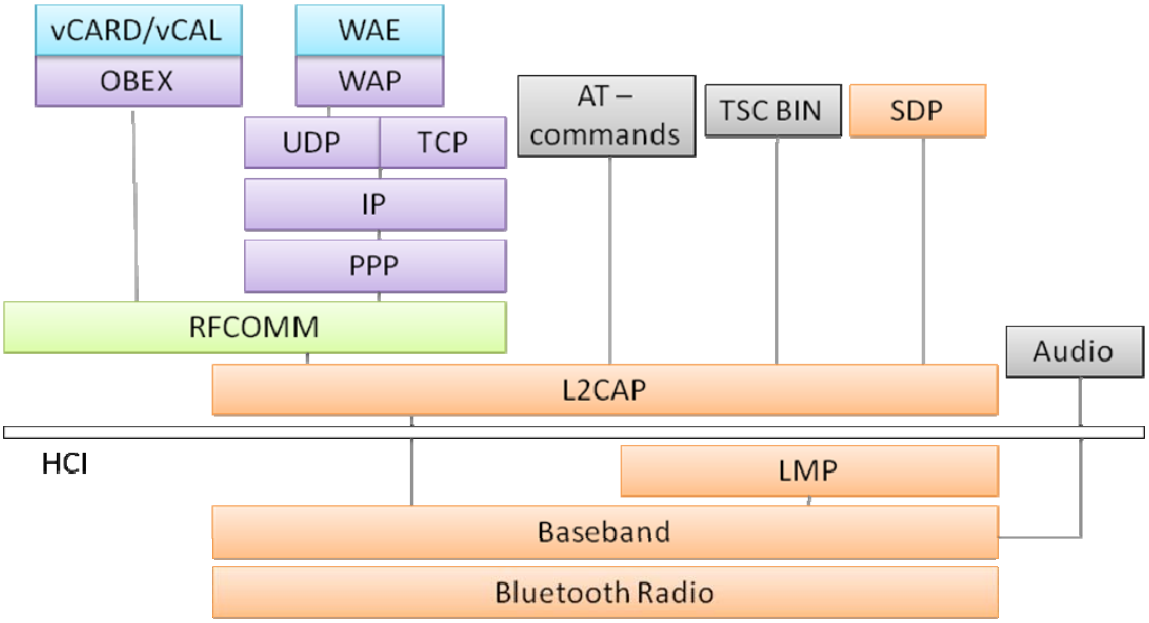
Posljednja objavljena specifikacija je „**Bluetooth low energy**“ koja je izdana 20. travnja 2009. godine. Neke od naprednih svojstava koje donosi ova inačica su:

- Kanali za višeodredišno razašiljanje (eng. broadcast) – omogućuje komunikaciju s informacijskim čvorovima.
- Upravljanje topologijom – omogućuje automatsku konfiguraciju Piconet topologije (mreža do 8 uređaja koji međusobno komuniciraju na načelu da se jedan ponaša kao gospodar te sinkronizira ostale).
- Poboljšanje QoS (eng. Quality of service) kvalitete – omogućen prijenos audio i video signala uz visoku kvalitetu.

2.3. Opis Bluetooth protokola

Bluetooth koristi mnoge protokole koje, kao i sam standard, definira organizacija Bluetooth SIG. Protokoli se dijele u četiri kategorije kako je prikazano na slici 2:

1. jezgreni Bluetooth protokoli (Bluetooth Radio, Baseband, LMP, L2CAP, SDP),
2. protokoli za zamjenu kabela (RFCOMM),
3. protokoli za nadzor telefonije (TSC BIN, AT commands),
4. preuzeti protokoli (PPP, UDP/TCP/IP, WAP, vCARD, vCAL, OBEX i drugi).



Slika 2 Bluetooth protokoli

2.3.1. Jezgreni protokoli

Jezgreni protokoli su sljedeći:

- **Bluetooth Radio** - protokol fizičkog sloja kojim se ostvaruje komunikacija između uređaja. Uređaji komuniciraju u nelicenciranom 2.4 GHz (2400 - 2483.5 MHz) ISM pojasu uz primjenu frekvencijskog skakanja. Definirana su dva načina rada:
  - obavezan način rada (eng. mandatory mode) koji se naziva „Basic Rate“ i
  - opcionalni način rada - „Enhanced Data Rate“.
- **Baseband** - rješava radijsku vezu dva uređaja. Predviđene su dvije mogućnosti:
  - sinkrona, spojno orijentirana veza prikladna za prijenos govora i
  - asinkrona, nespojna veza prikladna za prijenos podataka.
- **LMP** (eng. Link management protocol) protokol – koristi se za nadzor i uspostavu svih aspekata radio veze između dva uređaja. Ovo uključuje uspostavu i nadzor logičke veze, kao i provjeru fizičke veze. Sadrži podatkovne protokolne jedinice (eng. Protocol Data Units) koje nose informacije o:
  - nadzoru veze,
  - sigurnosti,
  - zahtjevima,
  - načinu rada,
  - logičkom prijenosu i
  - ispitivanju.
- **HCI** (eng. Host/Controller Interface) – standardizirana komunikacija između upravljačkih i poslužiteljskih slojeva. Postoji nekoliko različitih HCI transportnih slojeva, a svaki od njih koristi drugo sučelje za prijenos istih naredbi, događaja i podataka. Obično se koriste tehnologije USB (eng. Universal Serial Bus) kod osobnih računala te UART (eng. Universal asynchronous receiver/transmitter) kod mobilnih uređaja.
- **L2CAP** (eng. Logical Link Control & Adaptation Protocol)- protokol za nadzor veze i prilagodbu višim protokolima pružajući dijeljenje paketa, multipleksiranje i kvalitetu usluge.

  Postoje dva načina rada:

- ERMT (eng. Enhanced Retransmission Mode) – uključuje retransmisiju na L2CAP kanalu.
- SM (eng. Streaming Mode) – jednostavniji način rada bez retransmisije i provjere toka.

Temelji se na konceptu kanala, a svaka krajnja točka referencirana je s CID (eng. channel identifier) vrijednosti koja definira krajnju točku logičkog kanala na uređajima.

- **SDP** (eng. Service Discovery Protocol) – omogućuje uređajima otkrivanje usluga koje podržavaju drugi uređaji kao i parametara potrebnih za povezivanje s njima. Svaka usluga označena je s jedinstvenom UUID (eng. Universally Unique Identifier) oznakom.

2.3.2. Protokoli za emulaciju serijskih priključaka

Protokol za emulaciju serijskih priključaka **RFCOMM** (eng. Radio frequency communication) pruža emulaciju serijskih priključaka preko L2CAP protokola. Radi se o jednostavnom transportnom protokolu koji podržava do 60 simultanih veza između dva uređaja. Pruža stvarni prijenos niza podataka, a koriste ga mnogi Bluetooth programi zbog široke podrške (uporaba u pisačima, modemima i računalima). Omogućuje prijenos podataka „AT commands“ (naredbe za kontrolu uređaja), a može služiti i kao transportni sloj za OBEX.

2.3.3. Protokoli za nadzor telefonije

Protokoli koji se koriste za nadzor telefonije su:

- **TSC BIN** (eng. Telephony control protocol-binary) – protokol koji definira signalizaciju poziva za uspostave prijenosa govora i podataka između Bluetooth uređaja. Dodatno definira procedure upravljanja pokretljivošću uređajima.
- **AT commands** – skupina sučelja za komunikaciju s vanjskim aplikacijskim slojem.

2.3.4. Preuzeti protokoli

U skupinu preuzetih protokola uključeni su:

- **PPP** (eng. Point-to-Point Protocol) – standardni internetski protokol za prijenos IP datagrama preko „point-to-point“ veze. Spomenuta veza obično se koristi za povezivanje dvaju sustava preko WAN (eng. wide area network) mreža, a jedna od uobičajenih uporaba je razmjena podataka između lokalnog i udaljenog sustava.
- **UDP** (eng. User Datagram Protocol) – protokol koji omogućuje prijenos IP datagrama kroz Internetsku mrežu bez potrebe za uspostavom kanala.
- **TCP** (eng. Transmission Control Protocol) – protokol koji omogućuje prijenos niza podataka uz provjeru toka podataka, veličine segmenata i brzine prijenosa.
- **IP** (eng. Internet Protocol) – osnovni protokol koji omogućuje prijenos datagrama preko mreže pomoću adresa odredišnih čvorova.
- **WAP** – otvoreni standard koji korisnicima mobilnih telefona omogućuje uporabu telefonskih i informacijskih usluga.
- **vCARD** – jedan od formata sadržaja – elektronička posjetnica.
- **vCAL** – jedan od formata sadržaja – elektronički osobni kalendar s rasporedom aktivnosti.
- **OBEX** – sjednički protokol koji je razvila udruga IrDA (eng. Infrared Data Association) za jednostavnu i spontanu izmjenu objekata u modelu klijent – poslužitelj. U općem obliku radi se o pojednostavljenoj inačici HTTP (eng. Hypertext Transfer Protocol) protokola.

2.4. Usporedba s drugim bežičnim tehnologijama

U nastavku su navedene bežične tehnologije koje omogućuju prijenos podataka na kratkim udaljenostima.

UWB (eng. Ultra-Wideband) je tehnologija koja pruža jedinstvenu kombinaciju malog korištenja energije (~1mW/Mbps) i brzog prijenosa podataka (do 480 Mbps). Radi se o međunarodno priznatom standardu (ECMA-368, ISO/IEC 26970 i ECMA-369, ISO/IEC 26908). Obilježavaju ga niska uporaba energije, niska cijena, velika brzina, uporaba širokog radio spektra, prijenos signala kroz fizičke zapreke te primjena na razne aplikacije. Omogućuje prijenos na udaljenostima do 10 metara (dok Bluetooth omogućuje prijenos i do 100 m).

W/CWUSB (eng. Wireless/Certified Wireless USB) je standard osmišljen s ciljem postizanja velikih brzina prijenosa podataka (do 480 Mbps) na malim udaljenostima (2-10 m). Temelji se na UWB radio tehnologiji. Dizajniran je za rad u frekvencijskom spektru od 3.1 do 10.6 GHz (što čini osnovnu razliku u odnosu na Bluetooth tehnologiju), a koristi se u printerima, skenerima, MP3 uređajima i sl.

Wi-Fi (IEEE 802.11) je tip WLAN (eng. wireless local area network) mreže koji omogućuje uvođenje lokalnih mreža bez uporabe žica. Razvoj i ispitivanje provodi udruga „Wi-Fi Alliance“. Postoji više inačica standarda:

- 802.11a – koristi OFDM modulaciju te radi na frekvencijama od 5 GHz uz najveću brzinu prijenosa od 54 Mbps.
- 802.11b – radi na frekvencijama od 2.4 GHz uz najveću brzinu prijenosa od 11 Mbps.
- 802.11g – radi na frekvencijama od 2.4 GHz, koristi OFDM uz najveću brzinu prijenosa od 54 Mbps.
- 802.11e – standard koji donosi poboljšanje kvalitete usluga.
- 802.11h – standard pruža nadzor spektra i energije.
- 802.11i – standard donosi proširenje sigurnosti.
- 802.11k – standard donosi proširenje radio resursa, tj. korištenog frekvencijskog pojasa (još u razvoju).
- 802.11n – radi na frekvencijama od 5 GHz te pruža najveću brzinu prijenosa podataka preko 100 Mbps.
- 802.11p – radi na frekvencijama od 5.9 GHz.
- 802.11r – poboljšanje korisničkih mogućnosti za prijelazom s jedne priključne točke na drugu.
- 802.11s – standard omogućuje „mesh“ mreže u kojima se svaki čvor može ponašati kao neovisan usmjeritelj (još u razvoju).

Uvođenje Bluetooth tehnologije je financijski pogodnije jer zahtjeva tri puta manja ulaganja nego Wi-Fi sustavi. Također, korištenje energije kod Bluetooth uređaja je oko 5 puta manje nego kod Wi-Fi uređaja.

IrDA (eng. Infrared Data Association) standard pruža usluge bežične veze uređaja koji inače koriste kabel za međusobno povezivanje. Dizajniran je za udaljenosti do 1 m i brzine prijenosa od 9600 bps do 16 Mbps. Nedostatak ove tehnologije su potencijalno vrlo jake smetnje od djelovanja sunčeve svjetlosti ili fluorescentnih svjetiljki.

ZigBee (IEEE 802.15.4) je standard koji predviđa korištenje nelicenciranih pojaseva od 2,4 GHz i 900 MHz. Omogućuje domet od 10 do 75 m, a namijenjen je ponajprije za nadzor i upravljanje. U usporedbi s Bluetooth tehnologijom, brzine prijenosa podataka su dosta niže (do 250 Kbits).

Usporedba tehničkih značajki nekih od opisanih mreža dana je u tablici 2.

	Bluetooth	UWB	802.11b	802.11g	802.11a	802.11n	ZigBee
Propusnost (Mbps)	1-3	200	11	54	54	200	0,03
Najveći raspon (ft)	30	30	200	200	150	150	75
Energija (mW)	100	400	750	1000	1500	2000	30
BW (MHz)	1	500	22	20	20	40	0,6
Spektralna učinkovitost (b/Hz)	1	0,4	0,5	2,7	2,7	5	0,05
Cijena uređaja (US$)	3	7	5	9	12	20	2

Tablica 2 Usporedba bežičnih tehnologija

3. Ranjivosti i napadi

3.1. Sigurnost

Tijekom razvoja Bluetooth standarda uvedeni su brojni postupci i tehnologije kako bi se zaštitile komunikacije i prijenos podataka između Bluetooth uređaja. Neki od osnovnih razina i metoda zaštite navedeni su u nastavku.

Postoje četiri entiteta koji upravljaju sigurnošću na razini veze:

1. BD_ADDR (eng. Bluetooth device address) - adresa duga 48 bita koja jedinstveno određuje svaki uređaj, a definira ju organizacija IEEE (eng. Institute of Electrical and Electronics Engineers),
2. Privatni autentikacijski ključ (eng. Private authentication key) - slučajni broj duljine 128 bita koji se koristi za provođenje postupaka autentikacije.
3. Privatni ključ za kriptiranje (eng. Private encryption key) - broj dug 8-128 bita koji se koristi za šifriranje podataka.
4. RAND (eng. random number) - slučajni ili pseudo-slučajni broj duljine 128 bita koji se periodički mijenja, a stvara ga sam Bluetooth uređaj.

Bluetooth sigurnost dijeli se na tri razine:

- Razina 1 – nesigurna,
- Razina 2 – sigurnost na razini usluga,
- Razina 3 – sigurnost na razini veze.

Razlika između razine 2 i 3 je u tome što kod razine 3 uređaji iniciraju procedure sigurnosti prije uspostave kanala, dok se kod razine 2 to obavlja na razini usluge.

Što se tiče uređaja, definiraju se dva stupnja sigurnosti:

1. povjerljivi uređaj – neograničen pristup svim uslugama,
2. nepovjerljivi uređaj – ne postoji pristup uslugama.

Kod usluga postoje tri razine sigurnosti:

1. usluge koje zahtijevaju autorizaciju i autentikaciju,
2. usluge koje zahtijevaju autentikaciju,
3. usluge koje nemaju sigurnosnih zahtijeva.

3.1.1. Upravljanje ključevima

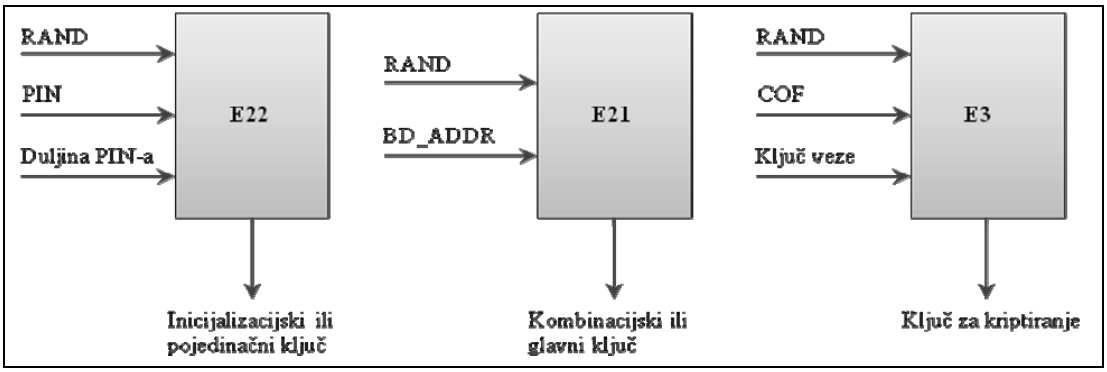
Svakim prijenosom podataka između uređaja rukuje se pomoću ključa veze. Radi se o slučajnom broju dugom 128 bita koji se koristi u procesu autentikacije kao parametar za stvaranje ključa za kriptiranje.

Postoji nekoliko vrsta ovog ključa:

- kombinacijski ključ (eng. combination key) – stvoren pomoću informacija iz oba uređaja u isto vrijeme preko algoritma E21 uz uporabu slučajnog broja i adrese uređaja.
- pojedinačni ključ (eng. unit key) – stvoren u jednom uređaju, a izračunava se preko algoritma E21 prilikom prve uporabe uređaja, nakon čega se pohranjuje u memoriju.
- glavni ključ (eng. master key) – privremeni ključ koji mijenja trenutni ključ veze, a stvara ga glavni uređaj (eng. master) uporabom dva slučajna broja duljine 128 bita. Dobiveni broj se šalje drugom uređaju kako bi se odredio trenutni ključ veze.
- inicijalizacijski ključ (eng. initialization key) – koristi se kao ključ veze tijekom inicijalizacije, prije nego se stvaraju kombinacijski i pojedinačni ključevi. Stvara se preko E22 algoritma koji koristi PIN broj, adresu uređaja i slučajni broj dug 128 bita. Duljina PIN vrijednosti može varirati između 1 i 16 okteta, a tijekom procesa inicijalizacije unosi se u oba uređaja.

Ključ veze se određuje iz trenutnog ključa veze, COF (eng. Ciphering Offset Number) vrijednosti i slučajnog broja dugog 128 bita preko algoritma E3. Ključ za kriptiranje se stvara

svaki put kada uređaj uđe u način rada za kriptiranje. Slika 3 prikazuje algoritme preko kojih se provodi stvaranje ključeva.



Slika 3 Algoritmi za stvaranje ključeva

3.1.2. Kriptiranje

Bluetooth sustav kriptiranja obavlja šifriranje paketa pomoću niza E0 koji se ponovno stvara za svaki novi podatak. Sastoji se od generatora ključa za nadopunu, generatora ključa niza i dijela za kriptiranje/dekriptiranje.

Generator ključa za nadopunu kombinira ulazne bitove i predaje ih LSFR (eng. Linear Feedback Shift Registers) registrima generatora ključa niza. Ovisno o uporabi ključeva postoji nekoliko načina kriptiranja. Ako se korisni pojedinačni ili kombinirani ključ, ne kriptira se promet koji se šalje na više odredišta, a individualni može ili ne mora biti kriptiran. Ako se koristi glavni ključ, postoje tri razine kriptiranja:

1. ne provodi se kriptiranje,
2. promet koji se šalje na više odredišta se ne kriptira, dok je individualni promet kriptiran glavnim ključem,
3. sav je promet kriptiran glavnim ključem.

Također, prije početka kriptiranja uređaji moraju dogovoriti duljinu ključa za kriptiranje putem parametra koji određuje najveću dopuštenu veličinu ključa za svaki od uređaja. Osim toga, svaki program ima definiranu najmanju potrebnu duljinu ključa pa može prekinuti „dogovaranje“ ključa ako nije moguće koristiti odgovarajuće kriptiranje. Ovo je potrebno u situacijama gdje bi zlonamjerni uređaji mogli inicirati uporabu slabog kriptiranja kako bi učinili neku veću štetu.

3.1.3. Autentikacija

Bluetooth shema za autentikaciju koristi strategiju „upit-odgovor“ kako bi se provjerilo zna li druga strana tajni ključ. Protokoli koriste simetrične ključeve pa se uspješna autentikacija temelji na činjenici da oba sudionika dijele isti ključ. U uređajima se računa i pohranjuje ACO (eng. Authenticated Ciphering Offset) vrijednost koja se kasnije koristi za stvaranje ključa.

U prvom koraku postupka autentikacije, jedan uređaj odabire slučajni broj i šalje ga drugom koji ga koristi za stvaranje SRES (eng. Signed Response) broja. Spomenuta vrijednost se dobije kao rezultat funkcije E1, koja za ulaz uzima odabrani slučajni broj, BD_ADDR drugog uređaja i ključ veze. Svaki uređaj računa SRES na isti način i iz istih parametara te provodi usporedbu. Ako pokušaj autentikacije nije uspješan, mora proći određeni definirani period vremena da bi se postupak ponovio.

Također, sami programi definiraju tko započinje autentikaciju te način njenog obavljanja (u jednom smjeru ili dvosmjerno).

3.1.4. Aspekt pokretnih mreža

U pokretnim mrežama postoji nekoliko mogućnosti osiguravanja prometa Bluetooth uređaja:

1. Uporaba kombinacijskog ključa za kriptiranje prometa – glavni uređaj definira kombinacijski ključ sa svakim ostalim uređajem u mreži te prenosi informaciju svim glavnim uređajima drugih mreža.
2. Uporaba koncepta glavnog ključa – svi uređaji koriste isti ključ kada kriptiraju pomet.

3.1.5. Problemi u sigurnosti

Neki od sigurnosnih problema koji su posljedica nedostataka opisane sheme kriptiranja su:

- E0 šifra duljine 128 bita može se otkriti u određenim situacijama sa složenosti $O(2^{64})$. Radi se o napadu „podijeli pa vladaj“ (eng. divide-and-conquer) koji je moguće izvesti ako je duljina ključa veća od perioda najkraćeg LFSR registra koji se koristi u stvaranju ključa s funkcijom E0. Ipak, ovaj je problem uključen u Bluetooth specifikaciju pa je napad gotovo nemoguće izvesti jer zahtjeva pristup ključu niza.
- Snaga stvorenog inicijalizacijskog ključa temelji se na korištenom PIN kodu jer se računa iz PIN-a, njegove duljine i slučajnog broja koji se prenosi zrakom. Tajnost izlaza je vrlo upitna jer je zasnovana na tajnosti PIN-a. Ako se koristi PIN kod s 4 znaka, postoji samo 10000 mogućih kombinacija. Uz činjenicu da je 50 % PIN vrijednosti jednako „0000“, povjerljivost inicijalizacijskog ključa je vrlo mala.
- Kod sheme pojedinačnog i kombiniranog ključa, autentikacija i kriptiranje se temelji na pretpostavci da je ključ veze dijeljena tajna informacija. Sve druge informacije koje se koriste u proceduri su javno poznate. Ako se dogodi da uređaji A i B koriste ključ uređaja A kao ključ veze, a u isto vrijeme isti ključ koriste i uređaji A i C, uređaj B može to iskoristiti za prisluškivanje prometa. Također, može se autenticirati uređaju A kao uređaj C ili obrnuto.
- Adresa uređaja, koja ga jedinstveno određuje, uzrokuje novi problem. Kada se odredi pripadnost jednog uređaja nekoj osobi, moguće je bilježiti sve transakcije te ugroziti privatnost osobe.
- Dodatni problem je mogućnost izvođenja napada uskraćivanja usluga (eng. Denial of Service). Rezultat ovog napada je nemogućnost korištenja sučelja uređaja te iskorištavanje energije baterije uređaja. Napad se obavlja stalnim slanjem zahtjeva sa jednog uređaja na drugim što iskorištava resurse i vodi do brze potrošnje energije. Ako napadač okupira vezu s posebno oblikovanim komunikacijskim zahtjevima dolazi do privremenog onemogućavanja usluge.

3.2. Povijest napada

Godine 2001. stručnjaci Jakobsson i Wetzel iz organizacije Bell Laboratories otkrili su propuste u protokolu za povezivanje uređaja (eng. pairing protocol) koji se koristi u Bluetooth tehnologiji. Također su ukazali na ranjivosti u shemi za kriptiranje.

U studenome 2003. godine Ben i Adam Laurie iz organizacije A.L. Digital Ltd otkrili su ozbiljne ranjivosti u sigurnosti Bluetooth tehnologije. Uspješnim iskorištavanjem tih propusta zlonamjerni bi korisnici mogli otkriti osjetljive podatke. Novi je napad nazvan BlueBug, a korišten je kao prezentacija pronađenih ranjivosti.

Prvi virus koji se širio putem Bluetooth tehnologije među mobilnim uređajima pojavio se 2004. godine na platformama Symbian OS. Spomenuti virus prva je opisala sigurnosna organizacija Kaspersky Lab koja navodi kako je potrebna korisnička potvrda za instalaciju tog zlonamjernog programa. Autori virusa su članovi skupine „29A“ koji su htjeli prikazati nepravilnosti u sigurnosti Bluetooth tehnologije.

U listopadu 2004. godine jedan je pokus pokazao kako je moguće proširiti doseg uređaja klase 2 na 1,78 km pomoću usmjerenih antena i pojačala signala. Ovo predstavlja potencijalnu sigurnosnu prijetnju jer omogućuje napadačima pristup ranjivim Bluetooth uređajima s veće udaljenosti nego se očekuje. Napadač mora imati mogućnost primanja informacija s ugroženog uređaja kako bi uspostavio vezu. Napad nije moguć ako napadač ne zna Bluetooth adresu i kanal za prijenos podataka.

Zlonamjerni crv pod nazivom „Lasco.A“ pojavio se na mobilnim uređajima koji koriste platforme Symbian OS. Koristio je Bluetooth uređaje za umnožavanje i širenje. Napad započinje kada

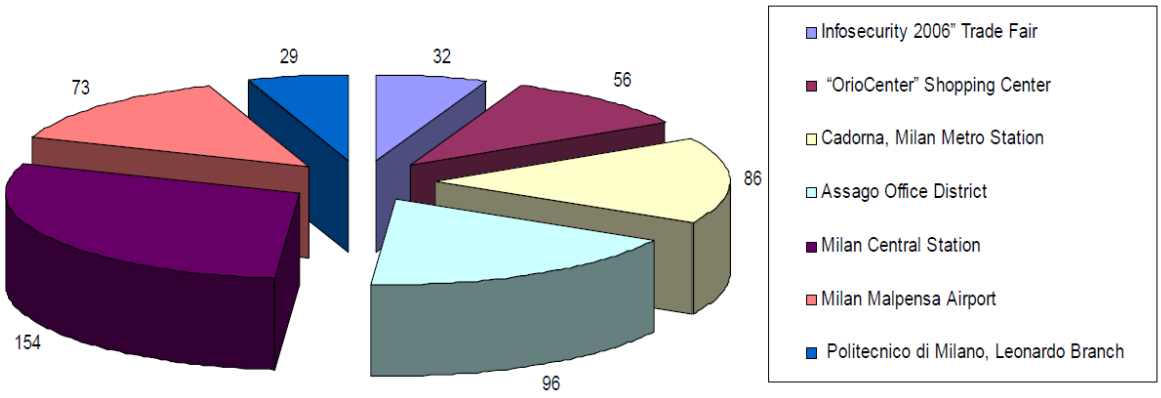
korisnik prihvati prijenos datoteke (velasco.sis) s drugog uređaja, a daljnje umnožavanje provodi samostalno. Kada je jednom instaliran, crv počinje pretragu za drugim Bluetooth uređajima koje može ugroziti. Dodatno, crv ugrožava drugu .sis (eng. Symbian Installation Source) datoteku ili prijenosni uređaj.

U travnju 2005. godine sigurnosni istražitelji sa sveučilišta „Cambridge University“ objavili su rezultate primjene pasivnog napada protiv spajanja preko PIN vrijednosti između Bluetooth uređaja. Ispitivanje je pokazalo da napad pogađa proceduru simetrične uspostave ključa pa se ukazuje na potrebu korištenja asimetrične procedure.

Yaniv Shaked i Avishai Wool su u lipnju 2005. godine objavili rad koji opisuje pasivne i aktivnu metode za otkrivanje PIN vrijednosti za uspostavljanje Bluetooth veze. Pasivni napad omogućuje prisluškivanje komunikacije ako je napadač prisutan u trenutku inicijalnog spajanja. Aktivna metoda koristi specijalno konstruirane poruke koje navode uređaje na ponavljanje procesa spajanja. Jedini nedostatak napada je zahtjev da korisnik pod napadom ponovi unos PIN vrijednosti.

U kolovozu 2005. godine policijski službenici u Engleskoj upozorili su na lopove koji uporabom uređaja s Bluetooth tehnologijom otkrivajudruge uređaje ostavljene u automobilima. Korisnici su upozoreni da moraju onemogućiti mobilne mrežne veze ako ostavljaju prijenosa računala i druge uređaje u automobilima.

Istražitelji sigurnosnih organizacija Secure Network i F-Secure objavili su izvješće koje upozorava na veliki broj uređaja koje korisnici ostavljaju „vidljivima“ (Slika 4). Također navode statističke podatke o širenju raznih Bluetooth usluga što pogoduje širenju virusa.



Slika 4 „Vidljivost“ Bluetooth uređaja
Izvor: securenetwork.it

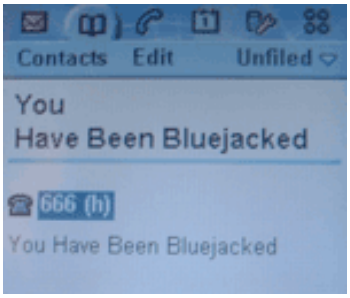
Na konferenciji Hack.lu u Luksemburgu u listopadu 2007. godine, Kevin Finistere i Thierry Zoller demonstrirali su prvi alat za otkrivanje PIN vrijednosti.

3.3. Najpoznatiji napadi

3.3.1. Bluejacking

Bluejacking je metoda slanja lažnih poruka preko Bluetooth standarda uređajima koji podržavaju Bluetooth tehnologiju poput mobilnih uređaja i prijenosnih računala. Lažne poruke su one koje nose primatelju nepotreban sadržaj, a služe u reklamne svrhe ili za ometanje korisnika. Napad se odvija slanjem vCard koji obično sadrži poruku u polju „name“, a prenosi se preko OBEX protokola. Obično uključuje uređaje klase 1, a omogućuje prijenos podataka brzinom do 1 Mbit/s na relativno kratkim udaljenostima (ne više od 10 m).

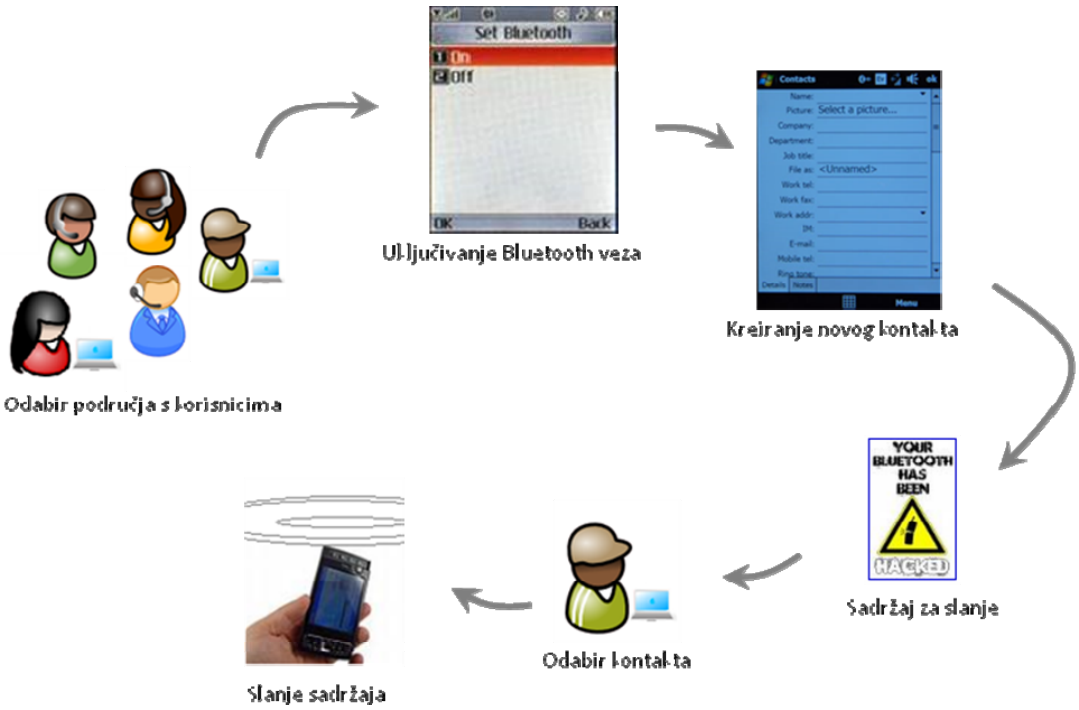
Prvi zabilježeni napad obavio je IT konzultant koji je koristio svoj telefon za reklamiranje firme Sony Ericsson. On je također odredio ime prema izrazu „jacking“ koji označava otimanje i preuzimanje stvari. Primjer rezultata jednog napada dan je na slici 5.



Slika 5 Primjer uspješnog Bluejacking napada
Izvor: lordpercy.com

Izvođenje napada uključuje sljedeće korake:

1. Odabir područja s mnogo korisnika Bluetooth uređaja,
2. Omogućavanje Bluetooth veza na vlastitom uređaju,
3. Kreirati novi kontakt (eng. Contact) i pripremiti sadržaj za slanje,
4. Aktiviranje funkcije slanja preko Bluetooth veze na adresu novog kontakta što pokreće skeniranje uređaja s omogućenim Bluetooth vezama,
5. Odabir jednog korisnika u popisu vidljivih uređaja te slanje pripremljenog sadržaja,
6. Primanje potvrde o uspješno poslanom sadržaju,
7. Ponavljanje postupka slanja poruka na isti/drugi uređaj.



Slika 6 Koraci Bluejacking napada

Ovaj oblik napada obično je bezopasan, ali značajni su jer napadnuti korisnici često misle kako im je telefon pokvaren. Napadači obično šalju tekstualnu poruku, ali na modernijim uređajima moguće je slati slikovne i audio zapise. Ponekad se koriste za promoviranje i reklamiranje proizvoda. Razvijeni su mnogi alati za obavljanje opisanog napada. Najveći dio razvoja dogodio se između 2000.-2004. godine kada su otkrivene mnoge nove Bluetooth ranjivosti. Većinu alata razvili su individualni programeri pa uključuju specifične funkcije.

Popis nekih alata koji omogućuju provođenje Bluejacking napada dan je u Tablica 3.

ALAT	PLATFORME	WEB STRANICA
SMan	P800/P900/P910i	~
Mobiluck	~	http://www.mobiluck.com/en/
Freejack	JAVA phones	~
ProximityMail	Pocket PC	http://www.inventop.com/
MeetingPoint	Pocket PC, Palm, Windows	~

Tablica 3 Alati za izvođenje Bluejacking napada

3.3.2. Bluesnarfing

Bluesnarfing je napad koji omogućuje neovlašteni pristup informacijama na uređaju (mobilnom uređaju, prijenosnom računalu i sl.) preko Bluetooth veze. To podrazumijeva pristup kalendaru, listi kontakta, porukama elektroničke pošte ili tekstualnim porukama, a na nekim uređajima i slikovnim te audio zapisima. Trenutno dostupni programi moraju dozvoliti povezivanje s drugim uređajima kako bi se omogućilo kopiranje sadržaja. Također napadač mora posjedovati odgovarajući program koji može ostvariti pristup uređaju.

Postoji jedna inačica Bluesnarfing programa koja je razvijena kako bi demonstrirala nedostatak u Bluetooth vezi između nekih mobilnih uređaja. Pronađena ranjivost ispravljena je u novijim inačicama Bluetooth standarda.

Opisani je napad mnogo ozbiljniji od Bluejacking napada iako oba iskorištavaju Bluetooth veze bez znanja korisnika. Svaki uređaj koji je uključen te ima postavljenu naredbu „*discoverable*“ (vidljiv drugim uređajima) može biti napadnut Bluejacking i Bluesnarfing napadom. Onemogućavanjem spomenute naredbe, potencijalne žrtve mogu osigurati veću razinu zaštite. Ipak postoje neke metode koje se mogu iskoristiti za napad na uređaje s funkcijom „*hidden*“ (skriven od drugih uređaja). Jedna od njih je pogađanje MAC (eng. Media Access Control) adrese uređaja putem „*brute force*“ napada (isprobavanje raznih kombinacija dok se ne otkrije odgovarajuća). Kao kod svakog napada tog tipa, glavna prepreka ovom pristupu je otkrivanje pravog broja adrese. Bluetooth koristi MAC adresu dugu 48 bita, od kojih prva 24 određuju proizvođača. Ostali bitovi daju oko 16,8 milijuna kombinacija, što zahtjeva oko 8,4 milijuna pokušaja da bi se pogodila ispravna adresa putem „*brute force*“ napada.

Važno je razlikovati napade Bluesnarfing i Bluejacking. Dok je Bluejacking napad u osnovi bezopasan i ne dovodi od otkrivanja podataka, Bluesnarfing omogućuje kopiranje žrtvinih podataka.

3.3.3. Bluesniping

Bluesniping se pojavio kao inačica Bluesnarfing napada, a označava jednostavno identificiranje uređaja koje podržavaju Bluetooth tehnologiju na većem rasponu nego je to dopušteno. Prema časopisu Wired Magazine, ova je metoda prvotno predstavljena na konferencijama Black Hat Briefings i DEF CON 2004. godine.

U travnju sljedeće godine, John Hering, student sveučilišta University of Southern California, razvio je uređaj „BlueSniper rifle“. Uređaj, prikazan na Slika 7, je koristio usmjerene antene, računalo opremljeno operacijskim sustavom Linux i Bluetooth modul. Imao je mogućnost otkrivanja Bluetooth uređaja na udaljenosti većoj od jedne milje (1,609 km).

Slika 7 Uređaj za izvođenje Bluesniping napada

Izvor: npr.org

3.3.4. Bluebugging

Bluebugging je oblik napada na Bluetooth uređaje koji je obično uzrokovan nedostatkom savjesnog ponašanja korisnika. Prvotno ga je uveo njemački istražitelj Herfurt 2004. godine. Njegov je program omogućavao zlonamjernim korisnicima da preuzmu nadzor nad žrtvinim telefonom. Drugim riječima, napadači mogu slušati razgovore korisnika u stvarnom vremenu. Dodatno, ovaj program omogućuje stvaranje programa za presretanje poziva kako bi napadač primio poziv umjesto svoje žrtve.

Inicijalno, napad je izvođen uporabom prijenosnih računala, ali danas je isti napad moguće izvesti s naprednim mobilnim uređajem. Cilj napada je upravljati zaštitom na uređaju kako bi se omogućilo izvođenje „*backdoor*" napada.

Daljnjim razvojem alata omogućeno je preuzimanje nadzora nad žrtvinim telefonom korištenjem slušalica za telefon koje napadač predstavlja kao slušalice žrtve. Time zavarava mobilni uređaj koji prepušta slušalicama naredbe pa napadač može ostvariti pozive, slati poruke, pregledati podatke i sl. Jedini problem leži u ograničenoj udaljenosti na kojoj je moguće izvesti napad. Drugim riječima, metoda je ograničena na prijenosnu snagu uređaja klase 2, tj. od 10-15 m. Ipak ovaj je raspon moguće povećati uvođenjem usmjerenih antena.

Napad može uzrokovati razne oblike štete za korisnika kao što je:

- otkrivanje povjerljivih podataka prisluškivanjem razgovora ili pregledom poruka,
- nanošenje financijskih troškova ostvarivanjem poziva ili slanjem poruka,
- otkrivanje telefonskog broja žrtve slanjem SMS (eng. Short Message Service) poruke na napadačev broj,
- lociranje korisnika putem ID vrijednosti u ćeliji (ovisno o operateru),
- otkrivanje korisnikovih poznanika pregledom popisa ostvarenih poziva,
- mijenjanje zapisa na uređaju (kontakti, popis poziva i sl.).

Najpoznatiji napad ovog tipa izveden je na uređajima Nokia 6310i Phone, a omogućen je nepravilnim uvođenjem Bluetooth standarda.

Neki od poznatijih alata dostupnih na Internetu prikazani su u Tablica 4.

ALAT	OPIS	WEB STRANICA
BlueSerial-Maemo	Alat za Nokia 770 Tablet PC	http://trifinite.org/Downloads/blueserial-maemo.tgz
Blooover	J2ME alat	http://trifinite.org/Downloads/Blooover.jar

Tablica 4 Alati za izvođenje Bluebugging napada

4. Zaštita i budući razvoj

4.1. Savjeti za zaštitu

Kako bi se zaštitili od opisanih napada korisnicima se savjetuje primjena sljedećih načela:

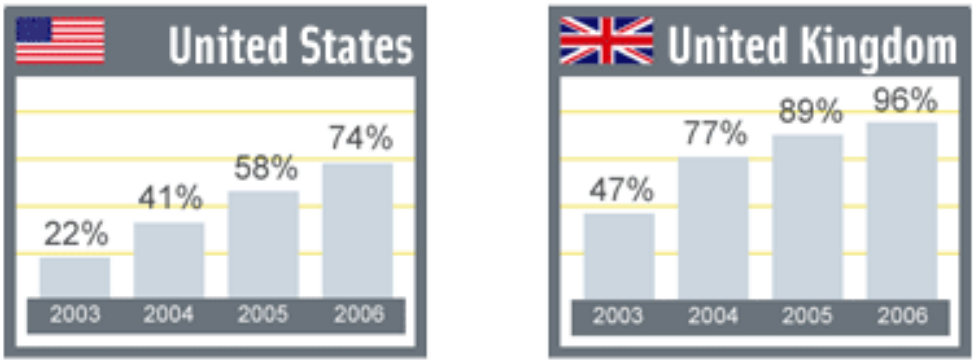
1. Općeniti savjeti
   - Usvajanje politike (http://csrc.nist.gov/publications/nistpubs/800-121/SP800-121.pdf) o bežičnoj sigurnosti koja se odnosi na Bluetooth.
   - Upoznavanje sa sigurnosnim problemima i odgovornostima.
   - Preuzimanje nadogradnje Bluetooth programa i operacijskog sustava za uređaje koju izdaju proizvođači.
   - Upoznavanje mogućnosti samog uređaja i povezivanja s drugim uređajima.
   - Promjena izvornih postavki uređaja (jer su one javno poznate te time i nesigurne).
   - Odabir slučajnog i dovoljno dugog PIN broja te izbjegavanje statičkih i slabih vrijednosti (poput „0000“) kako ih napadači ne bi mogli pogoditi ili otkriti „*brute force*“ napadom.
   - Gasiti Bluetooth uređaje kada se isti ne koriste kako bi se spriječilo njihovo korištenje za zlonamjerne radnje.
2. Savjeti vezani uz opcije uređaja:
   - Osigurati da se ključ veze temelji na kombinacijskom ključu, a ne na pojedinačnom kako bi se izbjeglo izvođenje MITM (eng. Man-in-the-middle) napada.
   - Postavljanje uređaja na najmanju potrebnu razinu energije (ako postoji navedena opcija) kako bi se prijenos omogućio u što je manjem mogućem rasponu.
   - Kod standarda Bluetooth 2.1 preporuča se uporaba naredbe „*Secure Simple Pairing*“ umjesto „*Just Works*“ kako bi se osigurala zaštita od MITM napadača.
   - Definirati korištenje samo onih usluga i profila koji su korisniku zaista potrebni.
   - Postaviti uređaje kao nevidljive drugim uređajima, osim u slučaju kada je potrebno povezivanje.
   - Imena za identifikaciju koja su izvorno postavljena potrebno je zamijeniti anonimnim imenima koje nije moguće povezati s korisnikom.
   - Definirati uporabu kriptiranja za sve Bluetooth veze kako bi se podaci zaštitili od prisluškivanja.
   - Zahtijevati uzajamnu (dvosmjernu) autentikaciju kod svih veza kako bi se provjerila legitimnost uređaja.
   - Omogućiti kriptiranje prometa koji se šalje na više odredišta.
   - Definirati uporabu što većih ključeva za kriptiranje koje dopuštaju uređaji i programi kako bi se zaštitili od „*brute force*“ napada.
   - Definirati najmanju potrebnu veličinu ključa za svaki proces „dogovaranja“ kako bi se spriječio odabir malog ključa koji nije otporan na „*brute force*“ napad.
   - Omogućiti uporabu autentikacije na razini aplikacijskog sloja jer uređaji mogu pristupiti ključu veze iz memorije na uređaju s kojim su prethodno ostvarili vezu.
   - Uključiti autentikaciju korisnika putem pametnih kartica ili PKI (eng. Public Key Infrastructure) infrastrukture što smanjuje opasnosti povezane s rukovanjem PIN-om.
   - Načini rada s manjom sigurnošću (razina 1 i 2) trebaju se koristiti samo u dobro poznatom okruženju.
3. Savjeti vezani uz ponašanje korisnika:
   - Izbjegavati primanje podataka s nepoznatih izvora i uređaja.
   - Instalirati antivirusni program na poslužitelje koji podržavaju Bluetooth tehnologiju kako bi se spriječili napadi raznim zlonamjernim programima.
   - Osigurati odgovarajuću zaštitu pristupa svih prenosivih uređaja koji podržavaju Bluetooth tehnologije kako bi se korisnici osigurali protiv krađe istih.

- U slučaju gubitka nekog od uređaja potrebno je prekinuti sve postojeće veze s tim uređajem kako bi se onemogućila daljnja komunikacija s ostalim uređajima.
- Izbjegavati upisivanje PIN broja u poruke koje to zahtijevaju osim u slučaju kada je zahtjev posljedica pokrenutog postupka povezivanja.

4.2. Očekivanja u budućnosti

4.2.1. Zainteresiranost i broj korisnika

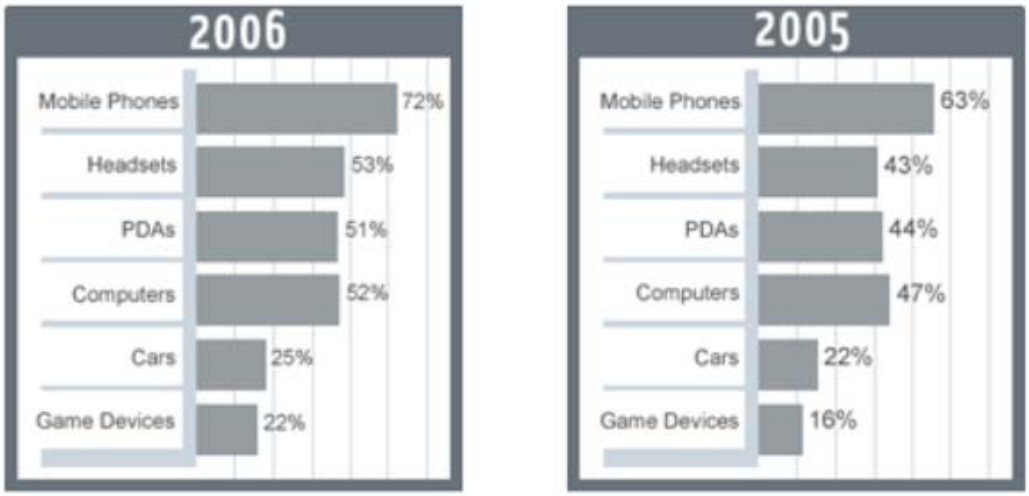
Prema izvješću jedne od vodećih svjetskih agencija za analize, Milward Brown, u prosjeku 81 % korisnika bilo je 2006.godine zainteresirano za Bluetooth tehnologiju (koriste ju ili žele koristiti). Posebno visoki interes primijećen je u Njemačkoj i Ujedinjenom Kraljevstvu (88-96%). Ostali podaci prikazani su na Slika 8.



Slika 8 Porast zainteresiranosti za Bluetooth tehnologiju

Izvor: bluetooth.com

Prema istom istraživanju, primjećuje se i zainteresiranost korisnika za uporabu Bluetooth tehnologije na pojedinoj vrsti uređaja. Posebno se veliki interes korisnika zamjećuje u slučaju mobilnih uređaja kako je vidljivo sa Slika 9.



Slika 9 Zainteresiranost prema vrsti uređaja

Izvor: bluetooth.com

Prema drugom istraživanju (pod nazivom „*Residential Technology Survey*“) organizacije In-Stat iz 2006. godine, vidljiva je povećana uporaba Bluetooth tehnologije. 2005. godine samo je 2 % ispitanika koristilo spomenutu tehnologiju, dok je 2006. godine taj broj iznosio 50 %.

Ako se uzmu u obzir navedeni statistički podaci, može se očekivati pojačan rast korisnika Bluetooth tehnologije i u budućim godinama. Zainteresiranost korisnika raste sve više u svim područjima uporabe tehnologije, što uključuje mobilne uređaje, slušalice, PDA uređaje, osobna računala, automobile i uređaje za igrice.

4.2.2. Razvoj tehnologije

Prema izvješću organizacije NPD Group, oko polovica svih mobilnih telefona prodanih u zadnjem kvartalu 2006. godine podržavala je Bluetooth tehnologiju. Isto istraživanje navodi kako je posjedovanje podrške za Bluetooth tehnologiju jedno od najpoželjnijih svojstava kod mobilnih uređaja.

Istraživanje organizacije In-Stat također navodi kako je Bluetooth tehnologija jedna od najbrže usvojenih tehnologija na GSM mobilnim uređajima. Također tvrde kako će se do kraja 2009. godine 66 % prodanih slušalica podržavati Bluetooth tehnologiju.

Organizacija Strategy Analytics objavila je kako je u 2005. godini prodano oko 33 milijuna slušalica te kako se može očekivati daljnje proširenje ovog tržišta.

Izvješće organizacije ISM donosi sljedeće zaključke:

- godine 2007. prodano je 7 milijuna automobila opremljenih s Bluetooth tehnologijom, a do kraja 2012. godine očekuje se da svaki treći auto ima uključenu ovu tehnologiju.
- prodaja automobila s ugrađenom Bluetooth tehnologijom se jako povećala pa se očekuje dostizanje prodaje do 40 milijuna kroz sljedećih nekoliko godina.
- primjećuje se velika popularnost uporabe ove tehnologije u uređajima za igrice.
- tržište audio opreme koja uključuje Bluetooth tehnologiju pokazuje rast od 2 milijuna primjeraka u 2005. godini do 9 milijuna u 2010. godini.
- uključivanje Bluetooth tehnologije u prijenosna računala ubrzano raste pa se očekuje da će oko 75% računala imati ugrađenu spomenutu tehnologiju do 2012. godine.
- očekuje se rast prodaje računala s Bluetooth tehnologijom s 14 milijuna u 2006. godini na oko 88 milijuna u 2012. godini.

5. Zaključak

Bluetooth tehnologija prisutna je u raznim programima i uređajima te čini jedan od bitnih aspekata komunikacije i prijenosa podataka između korisnika. Široku raširenost ova tehnologija može zahvaliti dobrim svojstvima poput brzog prijenosa podataka, mogućnosti stvaranja privremenih mreža, istovremene komunikacije s više uređaja i sl. Činjenicu o njenoj velikoj popularnosti potvrđuje i veliki broj korisnika, kao i stalni porast postojećih i uvođenje novih uređaja koji uključuju podršku za nju.

Iako omogućuje lak i jednostavan prijenos podataka i komunikaciju s bliskim uređajima, spomenuta tehnologija sadrži i određene sigurnosne probleme. Neke od ozbiljnijih prijetnji mogu korisniku nanijeti financijsku štetu ili omogućiti lažno predstavljanje napadača. Kako bi se osigurali od moguće krađe podataka ili upravljanja vezama i aktivnostima na uređaju, korisnicima se savjetuje savjesno rukovanje uređajima. Također, dodatnu zaštitu korisnici mogu osigurati preuzimanjem programske nadogradnje od proizvođača te pravilnim konfiguriranjem uređaja.

Kroz prethodne godine primijećen je veliki rast uporabe opisane tehnologije koja je uključena u mobilne uređaje, slušalice, prijenosna računala i dr. Prema tome može se očekivati daljnji porast popularnosti istih, te razvoj novih, naprednijih inačica Bluetooth standarda. Proširivanje funkcionalnosti i usluga koje nude uređaji opremljeni Bluetooth tehnologijom može uvesti dodatne sigurnosne rizike. Zbog toga se očekuje i uvođenje veće razine zaštite kao i ispravljanje do sada otkrivenih nepravilnosti.

6. Reference

[1] Bluetooth, http://en.wikipedia.org/wiki/Bluetooth, studeni, 2009.

[2] Bluetooth, http://www.palowireless.com/bluetooth/, studeni, 2009.

[3] Bluetooth, http://www.bluetooth.com/bluetooth/, studeni, 2009.

[4] Bluetooth, https://www.bluetooth.org/apps/content/, studeni, 2009.

[5] Bluetooth Radio, http://www.bluetooth.com/Bluetooth/Technology/Works/Architecture__Radio.htm, studeni, 2009.

[6] Bluetooth Baseband, http://www.bluetooth.com/Bluetooth/Technology/Works/Architecture__Baseband.htm, studeni, 2009.

[7] LMP, http://www.bluetooth.com/Bluetooth/Technology/Works/Architecture__Link_Manager_Protocol_LMP.htm, studeni, 2009.

[8] L2CAP, http://www.bluetooth.com/Bluetooth/Technology/Works/Architecture__Logical_Link_Control_and_Adaptation_Protocol_L2CAP.htm, studeni, 2009.

[9] RFCOMM, http://www.palowireless.com/infotooth/tutorial/rfcomm.asp, studeni, 2009.

[10] Usporedba tehnologija, http://www.bluetooth.com/Bluetooth/Technology/Works/Compare/, studeni, 2009.

[11] Bluejacking, http://en.wikipedia.org/wiki/Bluejacking, studeni, 2009.

[12] Bluesnarfing, http://en.wikipedia.org/wiki/Bluesnarfing, studeni, 2009.

[13] Bluesniping, http://en.wikipedia.org/wiki/Bluesniping, studeni, 2009.

[14] Bluebugging, http://en.wikipedia.org/wiki/Bluebugging, studeni, 2009.

[15] Juha T. Vainio, Bluetooth Security, http://www.mowile.com/bluesec.pdf, svibanj, 2000.

[16] Andreas Becker, Bluetooth Security & Hacks, http://gsyc.es/~anto/ubicuos2/bluetooth_security_and_hacks.pdf, kolovoz, 2007.

[17] Karen Scarfone John Padgette, Guide to Bluetooth Security, http://csrc.nist.gov/publications/nistpubs/800-121/SP800-121.pdf, studeni, 2009.

[18] Millward Brown Results 2007, http://www.bluetooth.com/Bluetooth/SIG/highlights/Millward_Brown_Results_2007.htm, 2007.

[19] Residential Technology Survey , http://www.instat.com/press.asp?ID=1704&sku=IN0602965MI, 2006.

[20] NPD Group, http://www.emarketer.com/Article.aspx?R=1004742, 2006.

[21] INDUSTRY STATISTICS, http://www.bluetooth.com/NR/rdonlyres/4E28B1F0-C1E3-419D-98EF-1DAC4C7A912D/0/IndustryStatSheet12.pdf, prosinac, 2007.

[22] Yaniv Shaked, Avishai Wool: Cracking the Bluetooth PIN, http://www.eng.tau.ac.il/~yash/shaked-wool-mobisys05/, svibanj, 2005.