Sigurnost bežičnih računalnih mreža

Mobilni internet

- Mobilni internet i bežični prijenos podataka imaju sve veću ulogu u svim aspektima mrežne komunikacije
  - prenose se različiti osobni i poslovni podatci,
  - komunicira se s prijateljima,
  - igraju se videoigre,
  - rade se različite simulacije,
  - održavaju se povjerljive poslovne videokonferencije i razgovori,
  - održava udaljena nastava,
  - provode financijske transakcije,
  - prenose povjerljivi vojni i državni podatci,
  - sklapaju različiti poslovi, potpisuju ugovori i sl.

Problemi u prijenosu

- U prijenosu podataka računalnom mrežom javljaju se različite pogreške koje mogu imati različite posljedice za sudionike u komunikaciji i resurse koje izmjenjuju podatkovnom mrežom.
- Do pojave pogrešaka može doći iz mnogih razloga:
  - kvarovi na korisničkim i mrežnim uređajima
  - propusti u programima
  - upotreba neažuriranih inačica programa
  - pristupanje nesigurnim web-mjestima
  - napadi od strane zlonamjernih korisnika
  - neovlašteni pristup od strane needuciranih ili neopreznih korisnika….

Napadi na bežične računalne mreže

- događaju se najčešće kako bi se ostvarila korist od napada na mrežu ili putem mreže na resurs
- Primjeri mogućeg **neovlaštenog pristupa bežičnim mrežama** su:
  - **ad hoc mreže** u kojima se komunikacija između dvaju ravnopravnih računala odvija izravno, bez pristupne točke (engl. peer-to-peer); **često se ne koriste metode zaštite** koje se mogu uvesti putem pristupne točke pa je sustav osjetljiviji na lažno predstavljanje, otkrivanje podataka i druge vrste napada
  - **netradicionalne mreže** (npr. Bluetooth) u kojima se zbog kratkog dometa komunikacije često **ne obraća dovoljno pažnje na sigurnost** pa otvaraju prostor napadačima za razna zlostavljanja
  - **slučajno povezivanje** (engl. accidental association) do kojeg može doći ako **se isti prostor koristi u više nezaštićenih bežičnih mreža** pa se korisnik može slučajno povezati s pogrešnom mrežom čime ugrožava sebe i tuđi sustav.

Primjeri napada

- **krađa identiteta** do koje može doći **ako podatci nisu šifrirani, a omogućeno je prisluškivanje** mrežnog prometa; tada napadač može saznati MAC (engl. Medium Access Control) adrese računala koja se koriste u lokalnoj mreži te upotrijebiti neki alat za **lažno predstavljanje** kao ovlašteni korisnik mreže
- **mrežno ubacivanje** (engl. network injection) je vrsta napada na cilj **radne postavke mrežnih uređaja** kao što su usmjernici i preklopnici i, a kojima se pristupa s WLAN-a s pomoću pristupne točke
- **zlonamjerno povezivanje** (engl. malicious association) izvode posebni programi koji **predstavljaju mrežnu karticu** napadača kao legitimnu pristupnu točku mreže napadača; posljedica uspješnog napada je **preusmjeravanje mrežnog prometa napadnute bežične mreže kroz računalo napadača**
- **napadi posredovanjem u komunikaciji** (engl. man in the middle) izvode se ako napadač ima podatke o uspješno izvedenom napadu zlonamjernog povezİvanja; tako dobiveni osjetljivi podatci mogu se koristiti za posredovanje u komunikaciji tako da **krajnji korisnici nisu svjesni da šalju i primaju podatke putem posrednika koji se lažno predstavio kao pristupna točka**

Sigurnosni mehanizmi standarda 802.11

- Podatci koji putuju bežičnom mrežom moraju biti zaštićeni od presretanja ili prisluškivanja te moraju doći nepromijenjeni na odredište.
- Najosnovniji ugrađeni sigurnosni mehanizmi standarda 802.11 su:
  SSID (engl. Service Set Identifier)
  provjera autentičnosti.
- SSID je identifikator, naziv koji opisuje koja se mreža pridružuje. Primjerice, svaki bežični usmjernik nosi naziv koji mu je namijenio proizvođač.
- *Često je to tip uređaja i broj serije kojoj pripada. Bilo bi dobro tu oznaku povremeno promijeniti pazeći da se u nazivu ne otkrije ime, prezime, adresa niti bilo koji drugi privatni podatak. SSID ili naziv Wi-Fi mreže može se promijeniti administratorskim sučeljem u koje se trebate prijaviti administratorskim vjerodajnicama. SSID može sadržavati do 32 znaka. Ako je mreža otvorena, svatko se može povezati samo sa SSID-om, a za sigurnije povezivanje potrebna je lozinka.*

Autentifikacija

- Da bismo dobili pristup mreži, prvo moramo proći postupak provjere autentičnosti.
- standardi koji definiraju provjeru korisnika:
  - **autentifikacija otvorenog sustava** omogućuje svima da se pridruže mreži i nema metode provjere autentičnosti
  - **autentifikacija zajedničkim ključem** temelji se na pretpostavci da obje strane u postupku provjere autentičnosti imaju zajednički ključ, a pretpostavlja se da je ključ proslijeđen klijentu na siguran način.

Bežični protokoli šifriranja prema standardu IEEE 802.11

- **WEP (engl. Wired Equivalent Privacy)** protokol šifrira podatke koji putuju između korisnika i pristupnih točaka sa zajedničkim ključem. Koristi algoritam sa 64-bitnim ključem, no pokazalo se da je takav sigurnosni mehanizam ranjiv i da ga je moguće probiti s pomoću javno dostupnih alata pa se ne preporučuje kao odgovarajuća mjera zaštite.
- Postoje dvije osnovne vrste napada na WEP: **pasivni** i **aktivni.**
- U pasivnim napadima napadač prisluškuje komunikaciju korisnika s mrežom prateći, na primjer, broj i veličinu paketa, ali **ne utječe na podatke** koje razmjenjuju pristupna točka i klijent.
- U aktivnim napadima **napadač aktivno utječe na podatke** i to može raditi na nekoliko načina: umetanjem svojih podataka, neovlaštenim korištenjem mrežnih resursa, gušenjem prometa na mreži, krivotvorenjem komunikacije klijenta i pristupne točke.

Ostali protokoli šifriranja

- **WEP2** je poboljšana inačica protokola WEP. Koristi algoritam sa 128-bitnim ključem. Kompatibilan je s WEP protokolom pa mrežna oprema zajedno s određenom nadogradnjom softvera može koristiti WEP2 protokol.
- **WPA-Personal**, poznatiji kao **WPA-PSK** (engl. Wi-Fi Protected Access-Pre Shared Key), način je na koji se naziva **unaprijed podijeljen ključ**, dizajniran za kućne i male uredske mreže, a **nije mu potreban poslužitelj za provjeru autentičnosti**. Svaki bežični mrežni uređaj šifrira mrežni promet izvodeći svoj 128-bitni ključ za šifriranje iz 256-bitnog zajedničkog ključa. Ovaj se ključ može unijeti ili kao niz od 64 heksadecimalne znamenke ili kao zaporka od 8 do 63 ASCII znaka.
- **WPA, WPA2 i WPA3** su inačice protokola za zaštitu bežičnih računalnih mreža nastale kao **odgovor na ozbiljne slabosti prethodnog sustava WEP protokola**. Inačica WPA2 usvojena je 2004. i zamijenila je inačicu WPA. Inačicu WPA2 zamijenila je 2018. inačica WPA3 koja koristi 192-bitni ključ za šifriranje.