Zaštita bežičnih mreža

Bežične mreže (IEEE 802.11 *wireless lan*) su zbog jednostavnosti postavljanja i lakoće pristupa bez potrebe za fizičkim transportnim medijem sve popularnije. Cijene bežičnih pristupnih točaka su sve niže, a mrežna sučelja za pristup bežičnoj mreži uglavnom dolaze kao standardna oprema u većini prijenosnih računala i drugih mobilnih uređaja. Kako bežične mreže svakim danom sve više ulaze u široku primjenu, važno je sagledati i sigurnosne aspekte korištenja bežičnih mreža, posebno zato jer ih jednostavnost pristupa čini dodatno izloženima na napade potencijalnih napadača.

Sigurnosne prijetnje

Sve sigurnosne prijetnje koje postoje u fiksnim mrežama su potencijalne prijetnje i u bežičnim mrežama, no zbog svoje izloženosti i jednostavnosti pristupa, u bežičnim mrežama postoje i dodatni sigurnosni rizici. Najveća prednost – bežični pristup – je ujedno iz sigurnosnog gledišta i najveći nedostatak bežične mreže. Signal kojeg emitira bežična pristupna točka nije moguće ograničiti samo na lokaciju gdje je fizički smještena organizacija unutar koje se poželjno da mreža bude dostupna. Maliciozni korisnici mogu dobiti pristup mreži prisluškivanjem prometa i probijanjem enkripcije ukoliko mreža nije adekvatno zaštićena.
Izraženije sigurnosne prijetnje bežičnim mrežama su:

- maliciozni korisnici mogu dobiti neautoriziran pristup internoj mreži kroz bežičnu mrežu,
- osjetljive informacije koje nisu kriptirane, a šalju se kroz bežičnu mrežu, mogu biti presretane,
- maliciozni korisnici mogu ukrasti identitet legitimnog korisnika i koristiti ga na mreži,
- moguće je izvršiti DoS (engl. *denial of service*) napad na bežičnu mrežu ili uređaj,
- maliciozni korisnici mogu kroz bežičnu mrežu pokretati napade na druge mreže, a da pri tome ostanu anonimni,
- maliciozni korisnik može postaviti pristupnu točku koja „glumi“ legitimnu pristupnu točku s ciljem da namami legitimne korisnike na spajanje na pogrešnu pristupnu točku.

Mehanizmi zaštite

IEEE 802.11 standard za bežične mreže predviđa mehanizme kojima je cilj povećanje sigurnosti bežičnih mreža odnosno ostvarivanja povjerljivosti i integriteta podataka te mogućnost sigurne autentikacije. Podaci koji putuju bežičnom mrežom moraju biti zaštićeni od presretanja ili prisluškivanja i moraju nepromijenjeni stići na svoje odredište.

WEP

Wireless Encryption Protocol (WEP) je protokol, dio IEEE 802.11 standarda, namijenjen osiguranju bežičnih mreža. WEP protokol kriptira podatke koji putuju između korisnika i pristupne točke zajedničkim ključem. Korisnik mora imati odgovarajući WEP ključ kako bi mogao komunicirati s pristupnom točkom. WEP protokol za enkripciju koristi RC4 algoritam s 64 ili 128 bitnim ključem, a za osiguranje integriteta podataka koristi se CRC-32 algoritam. Pokazalo se da je takav sigurnosni mehanizam moguće probiti javno dostupnim alatima i ne preporuča se kao odgovarajuća mjera zaštite.

WPA i WPA2

Wi-Fi Protected Access (WPA) je sigurnosni mehanizam osmišljen da ispravi nedostatke u WEP protokolu. WPA koristi dinamičke ključeve koji se mijenjaju za vrijeme korištenja sustava (TKIP) te „Michael“ algoritam za provjeru integriteta podataka. WPA2 kao dodatno poboljšanje umjesto RC4 koristi varijantu AES algoritma za enkripciju, ali nije podržan na starijim mrežnim sučeljima. Za autentikaciju, WPA podržava 802.1x, ali može se koristiti i manje sigurni sustav sa zajedničkim ključem – korisnici moraju poznavati zajednički ključ da bi se mogli spojiti na mrežu.

Zaključak

Bežične mreže uvelike povećavaju mobilnost korisnika i jednostavnost pristupa mreži, ali predstavljaju i nove sigurnosne rizike. Potrebno je procijeniti rizik mogućnosti bežičnog pristupa mreži i primijeniti adekvatan stupanj zaštite. Bežične mreže su dodatno izložene i time interesantne potencijalnim napadačima i osiguravanju treba pristupiti s pažnjom. Mehanizama zaštite bežičnog pristupa ima nekoliko, a neki od njih nisu dovoljno sigurni i mogu izazvati lažan osjećaj sigurnosti. Uz redovito praćenje razvoja tehnologije i primjenjivanje najsvježijih sigurnosnih mehanizama te kroz edukaciju korisnika i administratora, moguće je sigurnosne rizike svesti na minimum.