ZAŠTITA BEŽIČNIH MREŽA

Bežične mreže (IEEE 802.11 Wireless LAN) su zbog jednostavnosti postavljanja i lakoće pristupa bez potrebe za fizičkim transportnim medijumom sve popularnije. Cene bežičnih pristupnih tačaka (*Access Point*) su sve niže, a mrežni sistemi za pristup bežičnoj mreži uglavnom dolaze kao standardna oprema u većini prenosnih računara i drugih mobilnih uređaja. Kako bežične mreže svakim danom sve više ulaze u široku primenu, važno je sagledati i sigurnosne aspekte korišćenja bežičnih mreža, posebno zato jer ih jednostavnost pristupa čini dodatno izloženim na napade potencijalnih napadača.

Sigurnosne pretnje

Sve bezbednosne pretnje koje postoje u fiksnim mrežama su istovremeno i potencijalne pretnje i u bežičnim mrežama, ali zbog svoje izloženosti i jednostavnosti pristupa, u bežičnim mrežama postoje i dodatni sigurnosni rizici. Najveća prednost – bežični pristup – je ujedno sa bezbednosnog gledišta i najveći nedostatak bežične mreže. Signal koji emituje bežična pristupna tačka nije moguće ograničiti samo na lokaciju na kojoj je fizički smeštena organizacija unutar koje je poželjno da mreža bude dostupna. Zlonamerni korisnici mogu da dobiju pristup mreži prisluškivanjem saobraćaja i probijanjem enkripcije, ako mreža nije adekvatno zaštićena.

Izraženije bezbednosne pretnje bežičnim mrežama su sledeće:

- zlonamerni korisnici mogu da dobiju neautorizovan pristup internoj mreži kroz bežičnu mrežu;
- osetljive informacije koje nisu kriptovane, a šalju se kroz bežičnu mrežu, mogu biti presretnute;
- zlonamerni korisnici mogu da ukradu identitet legitimnog korisnika i dag a koriste na mreži;
- moguće je izvršiti DoS (engl. denial of service) napad na bežičnu mrežu ili uređaj;
- zlonamerni korisnici mogu kroz bežičnu mrežu da pokrenu napade na druge mreže, a da pri tome ostanu anonimni;
- zlonamerni korisnik može da postavi pristupnu tačku koja „glumi“ legitimnu pristupnu tačku, sa ciljem da namami legitimne korisnike na spajanje na pogrešnu pristupnu tačku.

Mehanizmi zaštite

IEEE 802.11 standard za bežične mreže predviđa mehanizme kojima je cilj povećanje bezbednosti bežičnih mreža, odnosno ostvarivanje poverljivosti i integriteta podataka i mogućnost sigurne autentifikacije. Podaci koji putuju bežičnom mrežom moraju biti zaštićeni od presretanja ili prisluškivanja i moraju nepromenjeni stići na odredište.

WEP

Wireless Encryption Protocol (WEP) je protokol, deo IEEE 802.11 standarda, namenjen osiguranju bežičnih mreža. WEP protokol kriptuje podatke koji putuju između korisnika i pristupne tačke zajedničkim ključem. Korisnik mora imati odgovarajući WEP ključ, kako bi mogao da komunicira sa pristupnom tačkom. WEP protokol za enkripciju koristi RC4 algoritam sa 64- ili 128-bitnim ključem, a za osiguranje integriteta podataka koristi se CRC-32 algoritam. Pokazalo se da je takav bezbednosni mehanizam moguće probiti javno dostupnim alatima i ne preporučuje se kao odgovarajuća mera zaštite.

WPA i WPA2

Wi-Fi Protected Access (WPA) je bezbednosni mehanizam koji je osmišljen da ispravi nedostatke u WEP protokolu. WPA koristi dinamičke ključeve koji se menjaju za vreme korišćenja sistema (TKIP) i „Michael“ algoritam za proveru integriteta podataka. WPA2 kao dodatno poboljšanje umesto RC4 koristi varijantu AES algoritma za enkripciju, ali nije podržan na starijim mrežnim sistemima. Za autentifikaciju, WPA podržava 802.1x, ali može da se koristi i manje sigurni sistem sa zajedničkim ključem – korisnici moraju da poznaju zajednički ključ da bi se mogli da se priključe na mrežu.

Zaključak

Bežične mreže uveliko povećavaju mobilnost korisnika i jednostavnost pristupa mreži, ali predstavljaju i nove sigurnosne rizike. Potrebno je proceniti rizik mogućnosti bežičnog pristupa mreži i primeniti adekvatan stepen zaštite. Bežične mreže su dodatno izložene i time interesantne potencijalnim napadačima i njihovoj bezbednosti bi trebalo pristupiti sa pažnjom. Postoji nekoliko mehanizama zaštite bežičnog pristupa, ali neki od njih nisu dovoljno sigurni i mogu da izazovu lažan osećaj sigurnosti.
Uz redovno praćenje razvoja tehnologije i primenu najsvežijih bezbednosnih mehanizama i naravno, kroz edukaciju korisnika i administratora, moguće je bezbednosne rizike svesti na minimum.