Seminarski Rad: Sigurnost Bežičnih Mreža

Marin Kurešić 3.b

Uvod

Sigurnost bežičnih mreža je ključna oblast u informacijskoj tehnologiji koja se bavi zaštitom podataka koji se prenose putem bežičnih komunikacijskih kanala. U današnjem digitalnom dobu, sveprisutnost bežičnih mreža čini ih atraktivnim ciljem za napade i ugrožavanje privatnosti i integriteta podataka. Ovaj rad će istražiti osnove sigurnosti bežičnih mreža, najčešće prijetnje s kojima se suočavaju te strategije i tehnike zaštite.

1. Osnove Sigurnosti Bežičnih Mreža

Sigurnost bežičnih mreža obuhvata niz tehnika i protokola koji se koriste za zaštitu podataka koji se prenose preko bežičnih veza. Osnovni koncepti uključuju:

- **Autentikacija**: Proces provjere identiteta korisnika ili uređaja koji se pokušava povezati s mrežom.
- **Autorizacija**: Proces odobravanja pristupa resursima mreže nakon uspješne autentikacije.
- **Šifriranje**: Tehnika koja se koristi za enkripciju podataka kako bi se osigurala privatnost i integritet.
- **Integritet podataka**: Provjera da li su podaci izmijenjeni ili oštećeni tijekom prijenosa.
- **Zaštita od napada**: Mjere koje se provode radi sprječavanja napada poput DoS (Denial of Service), Man-in-the-Middle, i brute force napada.

2. Prijetnje Bežičnim Mrežama

Bežične mreže su izložene raznim sigurnosnim prijetnjama koje uključuju:

- **Neovlašten pristup**: Napadači mogu pokušati pristupiti bežičnoj mreži bez odgovarajućih ovlaštenja.
- **Presretanje podataka**: Napadači mogu uhvatiti podatke koji se prenose preko bežičnih veza kako bi ih kasnije zloupotrijebili.
- **Ometanje usluge (DoS)**: Napadači mogu izvoditi napade kako bi onemogućili normalno funkcioniranje bežične mreže, sprječavajući legitimne korisnike da pristupe resursima mreže.
- **Napadi na autentikaciju**: Napadači mogu pokušati kompromitirati proces autentikacije kako bi stekli neovlašteni pristup mreži.

3. Strategije zaštite

Zaštita bežičnih mreža zahtijeva primjenu različitih strategija i tehnika kako bi se osigurala sigurnost i integritet podataka. Neki od ključnih aspekata zaštite uključuju:

- **Korištenje snažnih šifri**: Korištenje sigurnih i snažnih šifri poput WPA2 ili WPA3 za enkripciju podataka.
- **Autentikacija i autorizacija**: Implementacija mehanizama autentikacije poput WPA2-Enterprise ili korištenje EAP (Extensible Authentication Protocol) protokola za jaču sigurnost.
- **Segmentacija mreže**: Razdvajanje mrežnih segmenata kako bi se ograničio pristup osjetljivim resursima.
- **Redovito ažuriranje softvera**: Redovito ažuriranje firmware-a i softvera mrežnih uređaja radi ispravljanja sigurnosnih propusta i ranjivosti.

Zaključak

Sigurnost bežičnih mreža je od vitalnog značaja u današnjem digitalnom dobu. Razumijevanje osnovnih koncepta sigurnosti, identifikacija prijetnji i primjena odgovarajućih strategija zaštite ključni su koraci u osiguravanju sigurnosti bežičnih komunikacija. Kontinuirano praćenje sigurnosnih trendova i primjena najboljih praksi ključno je za održavanje integriteta i privatnosti podataka u bežičnim mrežama.