ZAŠTITA PODATAKA U RAČUNARSKIM MREŽAMA

U prošlosti se termin zaštita podataka obično vezivao za zaštitu podataka na izolovanim računarima. Međutim, pojavom računarskih mreža i njihovim stalnim razvojem i proširivanjem otvorila su se nova pitanja koja se tiču zaštite podataka koji se razmenjuju komunikacionim kanalima. Opasnost od ugrožavanja podataka je ovoga puta veća nego ikada ranije pre svega zbog fizičkih i funkcionalnih karakteristika računarskih mreža. Zbog toga je sadržaj ovog poglavlja posvećen zaštiti podataka u računarskim mrežama.

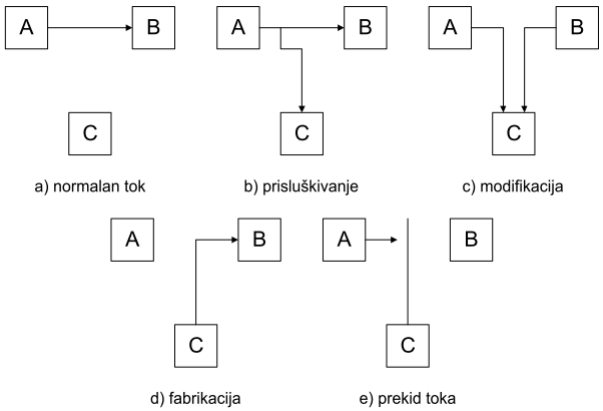
VRSTE NAPADA NA RAČUNARSKE MREŽE

Potencijalne pretnje podacima koji se transportuju kroz računarsku mrežu zasnivaju se na slabostima medija koji se koristi za transport podataka (bežična komunikacija, koaksijalni kabl, optički kabl i sl.), komunikacione opreme koja opslužuje računarsku mrežu, kao i softvera za mrežnu komunikaciju.

Ugrožavanje podataka u računarskim mrežama može biti višestruko i obično se odnosi na prisluškivanje, analizu, menjanje ili zadržavanje informacija, lažno predstavljanje itd. Ove nelegalne operacije mogu se izvesti na bilo kom mestu informacionog toka od izvora do odredišta. Na slici ispod prikazani su neki od mogućih napada na računarske mreže. U zavisnosti od uticaja potencijalnog napadača na tok informacija sve napade na računarske mreže možemo podeliti u dve grupe:

- Pasivni napadi (engl. passive attacks),
- Aktivni napadi (engl. active attacks).

Pasivni napadi se odnose na sve oblike prisluškivanja i nadgledanja toka informacija bez aktivnih izmena u samom toku. Na ovaj način napadač može doći do informacija koje se razmenjuju mrežom. Prisluškivanje koaksijalnih kablova je relativno lako izvodljivo uz pomoć elektromagnetnih senzora dok se prisluškivanje optičkih kablova ne može izvesti bez fizičkih intervencija na kablu pri čemu dolazi do slabljenja signala koji se može detektovati i na taj način sprečiti eventualni pokušaj prisluškivanja. Pasivne napade je u zavisnosti od konfiguracije mreže teško ali ne i nemoguće primetiti i onemogućiti, a kao najčešći mehanizam odbrane primenjuje se šifrovanje informacionog toka odnosno mrežnih paketa koji se distribuiraju mrežom.



Slika - Primeri napada na računarske mreže

Aktivni napadi podrazumevaju promenu sadržaja informacija ili njihovog toka. Jasno je da su zbog ove činjenice aktivni napadi mnogo opasniji i raznovrsniji od pasivnih. Napadač mora da bude direktno priključen na mrežu da bi izvršio ovakav napad bilo na komunikacionom čvoru ili na jednom delu komunikacionog toka. U aktivne napade svrstavaju se i modifikacija mrežnih paketa, fabrikacija neautorizovanih mrežnih paketa i prekid informacionog toka od strane napadača.