Pretnje i mere bezbednosti

dr Jasmina Novaković

1. PRETNJE I MERE BEZBEDNOSTI

- U ovom delu razmatra se uspostavljanje zaštićenih sistema koji su zasnovani na identifikaciji pretnji i analizi mogućih rizika, a posebno na ispitivanju određenih konkretnih napada na sistem i njegovo okruženje, verovatnoći ovih napada i gubicima do kojih oni mogu dovesti.
- Razmatraju se napadi na računarskoj mreži, bazama podataka i najčešće programerske greške koje mogu ugroziti sigurnost sistema.
- Analiziraju se mere zaštite koje obuhvataju prevenciju, detekciju i reakciju.
- Takođe, razmatraju se vrste bezbednosnih servisa: autentifikacija, privatnost, integritet podataka, servis kontrole pristupa, servis za onemogućavanje poricanja transakcije i raspoloživost resursa.

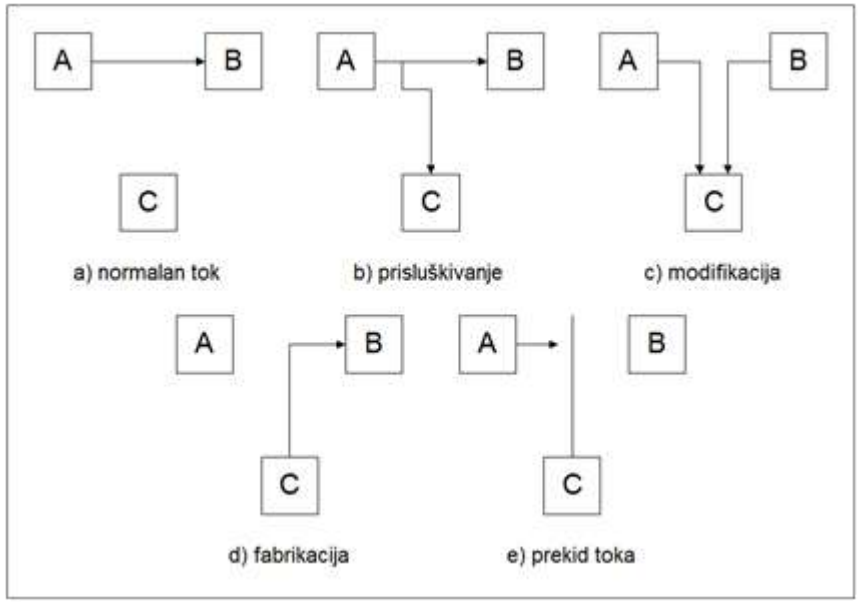
Nakon proučavanja ovog dela, trebalo bi da možete da:

- razumete potencijalne pretnje u računarskim sistemima;
- definišete moguće probleme u zaštiti računarskih sistema;
- analizirate mere zaštite;
- razumete osnovne bezbedonosne servise.

Pretnje sistemu

- Uspostavljanje zaštićenih sistema zasniva se na identifikaciji pretnji i analizi mogućih rizika, a posebno na ispitivanju određenih konkretnih napada na sistem i njegovo okruženje, verovatnoći ovih napada i gubicima do kojih oni mogu dovesti, na osnovu čega se identifikuju kritične komponente sistema.
- Sistem sam po sebi nije bezbedan, i u cilju zaštite informacija neophodno je u njega ugraditi određene zaštitne mehanizme, kao npr.: kontrola pristupa objektima u sistemu, šifrovanje informacija i sigurnosni protokoli.

Primeri napada na računarske mreže



Savremeni računarski sistemi moraju da obezbede:

- **Autentifikaciju** – Ko ste?
- **Autorizaciju** – Za šta ste ovlašćeni?
- **Pregled** – Šta ste uradili?
- **Integritet** – Da li je bilo šta u podacima neovlašćeno promenjeno?
- **Raspoloživost** – Da li je sistem/podaci/mreža raspoloživ(a)?
- **Poverljivost** (privatnost/tajnost) – Da li se može sačuvati tajnim?
- **Neporicanje slanja/prijema** – Ko je poslao/primio poruku?

Kriptologija

- Kriptografija predstavlja nauku o metodama i principima šifrovanja.
- Kriptoanaliza (ili razbijanje šifre - *codebreaking*) predstavlja nauku o metodama i principima dešifrovanja šifrovane poruke bez poznavanja ključa.
- Kriptologija kao nauka obuhvata i kriptografiju i kriptoanalizu.

Mere bezbednosti

- Upotrebom odgovarajućih mera bezbednosti mogu se izbeći rizici koje sobom nosi upotreba e-poslovanja.
- Samo ono e-poslovanje kod koje se koriste bezbednosne procedure u skladu sa procenjenim rizicima predstavlja bezbedno e-poslovanje.

Mere zaštite obuhvataju:

- prevenciju,
- detekciju,
- reakciju.

Autentifikacija omogućava utvrđivanje identiteta korisnika:

- nečim što samo korisnik zna, kao što je lozinka;
- nečim što samo korisnik ima, kao što je kartica ili žeton;
- nečim što samo korisnik jeste, kao što je potpis, glas, otisak prsta, snimak oka, geometrija šake, fotografija lica i slično, što se sprovodi biometrijskim kontrolnim sredstvima.