UVOD

Kroz implementaciju sigurnosnih standarda u virtuelnim privatnim mrežama izložena su osnovna načela, tehnike i postupci zaštite informacija kao odgovor na pitanje sigurnosti protoka informacija putem nesigurne javne mrežne infrastrukture, kao što je Internet.
Upoznaćemo se sa konceptom virtuelnih privatnih mreža, kao tehnologijom koja obuhvata sve pojedine postupke zaštite informacija na njihovom cijelom putu, od pošiljaoca do primaoca. Govorim o potrebama za nastajanjem i razvojem virtuelnih privatnih mreža i prednostima koje pruža, naručito u današnjem komercijalnom svijetu, sve prisutnosti Interneta i nezaustavljivom tehnološkom razvoju.

Kroz rad su izložene osnovne tehnike enkripcije, autentifikacije i enkapsulacije koje omogućavaju da podaci u transportu kroz dijeljenu infrastrukturu, od svog polazišta do cilja, budu neupotrebljivi bilo kome drugom sem osobama kojima su prvenstveno i namjenjene, bez obzira na činjenicu da su na javnoj mreži vidljive svima.
S obzirom na danas sve češće i raznovrsnije napade na mreže resurse, postavlja se pitanje kako obezbjediti povjerljivost, integritet i raspoloživost podataka, kao bazna svojstva svake kvalitetnije zaštite informacija. Treba razmotriti i pitanja autentifikacije, autentičnosti i autorizacije.

Šifriranjem podataka, čineći ih na taj način nečitljivima bez odgovarajućih podataka za dešifrovanje, postiže se povjerljivost tih podataka. Zato su u trećem poglavlju opisani osnovni pojmovi vezani za šifriranje, razvoj i opis osnovnih algoritama koji se koriste u tu svrhu i koji su identiteta pošiljaoca kroz tehnike kao što su digitalni prihvaćeni kao standardi.
Sljedeći nivoi u zaštiti informacija je obezbjeđivanje njihovog integriteta i autentičnosti, što potvrđuje da su podaci na cilj stigli cjeloviti, neizmjenjivi i iz autentičnog izvora. Ovdje se izlažu osnovni principi i standardni algoritmi za razmjenu tajnih dijelova šifriranih poruka, te potvrdu potpisi i certifikati.

Zatim je opisan način sigurnog prijenosa zaštićenih paketa kroz javnu mrežu putem tuneliranja, kroz čiju transparentnost se opravdaju aspekti virtualnosti i privatnosti tehnologije virtuelnih privatnih mreža. Način obezbjeđivanja blagovremenog stizanja poruka na odredište je takođe objašnjeno.

Na kraju je opisana praktična situacija u kojoj se primjenjuje virtuelno privatno umrežavanje, kao sveobuhvatno rješenje sigurnog elektronskog poslovanja putem prostornog Interneta, te u cilju uspostavljanja takve konekcije, ponuđena softverska i hardverska rješenja, razmatrane njihove razlike, prednosti i nedostaci.

Ovaj kratak pregled Implementacije sigurnosnih standarda u virtuelnim privatnim mrežama, imao je za cilj da ukaže na njenu sveobuhvatnost i sistematičnost, te značaj primjene u današnjem tehnološkom svijetu, naručito u elektronskom poslovanju. Opis tehnika i alogoritama za zaštitu, te načina transporta podataka do odredišta, trebao je uvjeriti svakoga u navedene prednosti tehnologije virtuelnog privatnog umrežavanja.