

Uvod u informaciono-komunikacione tehnologije

S. Stamenković. Autor, copyright ©2010., E-mail: office@sasastamenkovic.com, URL: <http://www.sasastamenkovic.com/blog>

Članak sadrži kratak osvrt na istoriju razvoja informaciono – komunikacionih tehnologija. U radu se mogu naći odgovori na pitanja koji se tiču razvoja digitalnih tehnika generisanja signala, razvoja protokola i konačno primene kriptografskih metoda zaštite digitalnih podataka na Web-u.

Ključne reči — Informaciono-komunikacione tehnologije, kriptografija, TCP/IP, NCP, virtuelne mreže, komutiranje.

I. UVOD

NASTANAK informaciono-komunikacionih tehnologija je u bliskoj vezi sa razvojem i integracijom telekomunikacija i teorije informacija [1]. Dostignuća na polju razvoja digitalnih tehnika generisanja, obrade i prenosa signala u je imala i ima veliki uticaj i na učestalost promena u sveri savremenog informatičkog društva. Informatičko društvo je u pojedinim fazama razvoja imalo tendenciju da postane, a danas se može i smatrati stubom razvoja celokupnog društva budući da povezuje sve privredne grane, znanja i dostignuća ljudi u svim oblastima. Razvoj civilizacije, posmatrano sa istorijskog aspekta svedoči o postepenom prikupljanju znanja koja su potom klasifikovana. Znaja od posebnog značaja za čoveka su ne retko izdvajana, a u nekim slučajevima, određene vredne informacije i dostignuća su svoj put pronašle u zatvorenim krugovima. Pojedini vredni resursi su neretko bili u službi onih koji su razumeli njihov značaj i imali pristupa. Vrednost pojedinih informacija je zahtevala dodatne mere zaštite integriteta. Nastala je i kriptografija kao specijalizovana disciplina u službi tajnosti informacija. Značajniji pomak na polju razvoja ove discipline zabeležen je 1918. godine pošto je objavljena čuvena Monografija William-a F. Friedman-a [2] koja sadrži izveštaj o istraživanjima u privatnim laboratorijama Riverbank. Iste godine Edward Hebern je prvi prijavio patent za rotator mašinu koji je postao osnova vojne kriptografije tokom približno 50 godina. Dalji razvoj u ovoj oblasti preneo se i u sferu informacionih tehnologija, razvijeni su brojni standardi i algoritmi za kriptovanje koji se danas uspešno primenjuju u cilju zaštite integriteta informacija na Webu. Većina algoritama za kriptovanje je danas integrisana u popularnim programskim jezicima kao što su PHP, C, C++, Delphi, ASP itd.

Decentralizacija mreža računarskih resursa, šezdesetih godina prošlog veka bila je okosnica interesovanja mreže ARPAnet-a [3]. Na ovaj način postiglo se da pristup i korišćenje računarskih resusa postane potpuno nezavisan sistem koji opstaje i funkcioniše bez obzira na to da li neki računar u mreži funkcioniše ili ne... Takva tipologija mreža zasnovana je na pricipu čvorišta, a informacija do krajnjeg računara stiže sve dokle postoji putanja koja povezuje čvorove mreže, pa se ne retko kaže da je ovo “mreža svih mreža”[4] koja može izdržati i atomski udar. Sa druge strane značajnija promena na polju razvoja Internet tehnologija se zasniva na primeni komutiranja paketa, na manje celine, koje se potom ponovo sklapaju u celovitu formu.

Prvobitni NCP [5] iz 1982. je kasnije zamenjen kombinovanjem TCP/IP koji je omogućio međusobno povezivanje mreža. Konačno, ovako povezani računari koji sada mogu nesmetano komunicirati ostvarujući pritom virtuelne veze i kao takvi, trebaju koristiti u službi znanja i informisanja... Znanje i informacije u obliku zapisa moraju biti zabeležene i fizički prisutne u bazama podataka i posebno organizovane u odgovarajue tabele relacionih baza što danas čini osnov modela troslojne arhitekture na Webu, a samim tim i osnov “drugog talasa Web-a” (Web 2.0).

LITERATURA

- [1] Teorija informacija bavi se definicijom mere količine informacija; proučavanjem izvora informacija; proučavanjem prenosnog kanala, analizom granica koje optimalni sistem može dostići, konstrukcijom prenosnog sistema što boljih performansi...
- [2] W. Friedman, The index of Coincidence and its Applications in Cryptography, 1918.
- [3] Advanced Research Projects Agency Network: radilo se o manjem istraživačkom timu na Institutu za Tehnologiju u Massachusetts, SAD.
- [4] S. Obradović, “Osnovi računarske tehnike“, str.405, avgust 2005.
- [5] Network Control Protocol
- [6] Reč je o dostignuću ARPAnet-a koje se zasniva na prenosu podataka između dva sistema u obliku niza paketa, pri čemu se svaki od ovih paketa šalje kao zasebna celina.