PRIMERI SISTEMA ZAŠTITE PODATAKA U RAČUNARSKIM MREŽAMA

KERBEROS

Kerberos predstavlja sistem za autentifikaciju u otvorenim sistemima i mrežama. Razvijen je na Institutu za tehnologiju u Masačusetsu (Massachusetts Institute of Technology). Kerberos se može implementirati u bilo koji postojeći mrežni protokol a koristi sistem za šifrovanje koji je baziran na DES (Data Encryption Standard) sistemu šifrovanja. Svaki korisnik poseduje svoj ključ za autentifikaciju. Kerberos čuva podatke koji se prenose kroz računrsku mrežu između dva računara. Ovaj sistem koristi kriptografske ključeve poznatije kao kartice (tickets) za zaštitu poruka koje se transportuju kroz mrežu. Kerberos ni u jednom slučaju ne vrši transport lozinki kroz mrežu, čak ni u šifrovanom stanju. Lozinke se nalaze samo na jednom, veoma sigurnom računaru koji se naziva server za ključeve (key server). Autentifikacija se vrši kako pri logovanju na sistem tako i pri zahtevu za izvršenje nekog od mrežnih servisa. Ovaj sistem implementiran je i na delu univerzitetske računarske mreže u Beogradu.

PROJEKAT MAX (PROJECT MAX)

Ovaj projekat je urađen od strane mnogih komercijalnih ponuđača uključujući tu i SecureWare, Sun i Hewlett-Packard. Cilj projekta je bio razvoj sigurne mrežne tehnologije koja je nezavisna od proizvođača hardverske platforme, specifičnog operativnog sistema i mrežnih protokola. To bi omogućilo sigurnu razmenu podataka između različitih računarskih sistema i mreža.

Ova grupa proizvođača razvila je proizvod pod nazivom MaxSix (Multilevel Architecture for X for Security Information Exchange). MaxSix sačinjava skup poboljšanja UNIX operativnom sistemu i mrežnom MTVU lekcijekomuniciranju. Posebna pažnja posvećena je standardizaciji označavanja podataka koji se unose i iznose iz sistema.

MaxSix je razvijen tako da podržava sigurnosne mrežne standarde uključujući tu i DNSix i TSIG. DNSix je razvijen od strane DIA (Defense Intelligence Agency) dok je TSIG (Trusted Systems Interoperability Group) razvio specifikaciju za zaglavlja poruka koja uključuju atribute kao što su na primer oni za označavanje osetljivosti podataka koji se transportuju mrežom.

SDNS (SECURE DATA NETWORK SYSTEM)

Ovaj sistem zaštite podataka u računarskim mrežama razvijan je od strane američke NSA (National Security Agency) a u njega je uključeno deset velikih američkih kompanija. Između ostalih u projektu su učestvovali i AT&T, DEC (Digital Equipment Corporation) i IBM. Cilj ovog projekta je bio da se razvije zaštitna arhitektura bazirana na OSI modelu.

SECURE NFS

Proizvod firme Sun Microsistems NFS (Network File System) predstavlja skup mrežnih protokola koji su postali industrijski standard za UNIX operativne sisteme. NFS omogućava klijent sistemu (radna stanica) da montira uređaj na fajl serveru baš kao da je server fizički priključen na sistem. Ovaj sistem koristi dva tipa šifrovanja: prvi je DES (Data Encryption Standard) koji spada u simetrične sisteme šifrovanja, a drugi je sistem javnih ključeva.