SADRŽAJ:

1. Uvod

Kontrola pristupa je dio sigurnosne politike koja je prisutna u gotovo svakom operativnom sistemu. Mehanizmi kontrole pristupa ograničavaju korisnike i procese u smislu izvođenja različitih operacija nad objektima, kao što su datoteke, dijelovi zajedničke memorije... Za svaku takvu akciju mehanizmi kontrole pristupa dodjeljuju svakom korisniku posebna prava za obavljanje određenih akcija na računaru. Navedeni mehanizmi kontrole pristupa prisutni su u nekoliko slojeva, od aplikacijskog sloja preko operativnog sistema, pa sve do hardvera. Mehanizmi viših slojeva su više izraženi, ali su i podložniji napadima. Neki od razloga su složenost sistema i programerske pogreške. Programi i operativni sistemi mogu biti vrlo složeni te time uzrokuju pojavu propusta u bezbjednosti cjelokupnog sistema. Kontrola pristupa ima ulogu ograničavanja štete koju napadači ili neoprezni korisnici mogu prouzročiti.

Kontrola pristupa dijeli se prema metodama implementacije na:

• diskrecioni model (samovoljna kontrola pristupa) (DAC – Discretionary Access Control),
• mandatorni model (obavezna kontrola pritupa) (MAC – Mandatory Access Control) i
• model grupa i uloga (kontrola pristupa bazirana na ulogama) (RBAC – Role-based access control).

2. Modeli kontrole pristupa

Kontrola pristupa definiše mehanizam dozvole ili zabrane pristupa računarskim procesima i različitim računarskim resursima, a osim toga omogućava nadzor nad sistemom u smislu uvida u aktivnosti prijavljenih korisnika te na kraju vođenja evidencije o ostvarenim pristupima svih registriranih korisnika (log). Osnovni problem sigurnosti je nadzor nad situacijama u kojima neki korisnik ili program smije pristupiti nekom objektu u određenom trenutku i na koji način to smije izvesti. Pristup nekom resursu, definiše kakve se akcije i operacije smiju obavljati nad određenim objektima. Na primjer, mogu to biti čitanje datoteke, pisanje u datoteku, stvaranje ili brisanje objekata, povezivanje sa nekim drugim programom, itd.

U smislu razmatranja kontrole pristupa, uzimaju se u obzir četiri situacije:

• sprječavanje pristupa – potrebno je osigurati da jedan korisnik ne može nanijeti štetu i narušiti integritet podataka nekog drugog korisnika na istom računarskom sistemu,
• ograničavanje pristupa – potrebno je osigurati da korisnik nema pristup nekim ključnim resursima kojima bi trebao moći pristupiti samo administrator sistema,
• dozvola pristupa – dozvoljavanje prijenosa određenih prava pristupa s jednog korisnika na drugog,
• oduzimanje prava pristupa – treba omogućiti oduzimanje već dodijeljenih prava pristupa.

pristupa uz uslov pozitivne autentifikacije-dokazani identitet).