SUSTAVI KONTROLE PRISTUPA

Aleksandar Pašagić

Sustavi kontrole pristupa doživjeli su značajan napredak u relativno kratkom vremenskom razdoblju, kako u vidu korištenih tehnologija, tako i po pitanju njihove rasprostranjenosti. Od danas već staromodnih kartica s magnetskom trakom, pa sve do biometrijskih čitača, niti jedna firma, ustanova ili organizacija koja drži do svoje sigurnosti i povjerljivosti ne može se zamisliti bez nekog sustava kontrole pristupa.

Principi djelovanja

Iako kontrola pristupa u širem smislu podrazumijeva sposobnost da se specifičnom subjektu omogući ili onemogući uporaba određenog resursa, te se po toj definiciji proteže i na upravljanje logističkim i digitalnim resursima poput pristupa bankovnom računu ili određenom dokumentu na nekom računalu ili računalnoj mreži, u ovom članku koncentrirat ćemo se na fizičku kontrolu pristupa, s naglaskom na novije tehnologije koje se koriste u tu svrhu. Samo ćemo napomenuti da i „jednostavnije“ metode, poput čuvara na vratima ili staromodnog lokota također spadaju u kontrolu pristupa, te da još uvijek imaju svoju legitimnu primjenu ovisno o specifičnosti situacije.
Većina sustava kontrole pristupa zamišljena je sa svrhom da određenim pojedincima dopusti prolaz kroz određenu zaustavnu točku, a da taj isti prolaz drugima onemogući. Kako bi se to moglo ostvariti, mora postojati sustav koji će „poželjnog“ pojedinca identificirati kao takvog. Ta identifikacija sprovodi se na način koji se može svrstati u jednu od tri kategorije:
- identifikacija pomoću nečega što pojedinac posjeduje; to uključuje fizičke objekte poput magnetnih ili digitalnih kartica;
- identifikacija pomoću znanja specifičnog za pojedinca ili pogodnu skupinu ljudi, kao što su lozinke ili niz brojeva pomoću kojih se dobiva pristup, deaktivira alarmni sustav ili slično; te
- identifikacija pomoću svojstava specifičnih za točno određenu osobu, odnosno biometrijskih karakteristika, kao što su otisak prsta ili glasovni uzorak.

Ključne komponente sustava kontrole pristupa svode se na:
- uređaje za potvrđivanje, kao što su, na primjer, kartica i čitač kartica;
- uređaje koji fizički zaključavaju vrata, odnosno na neki drugi način onemogućuju prolaz ukoliko se ne zadovolje uvjeti koje diktiraju uređaji za potvrđivanje;
- kontrolni uređaj koji donosi odluke o dopuštanju pristupa u odnosu na informacije dobivene od uređaja za potvrđivanje;
- programski paket pomoću kojega se sustav izvorno programira, te kojim se mogu implementirati promjene u kriterijima za dopuštenje pristupa.

Pristupne kartice i čitači kartica

Pristupne kartice i pripadni čitači najočitiji su dio sustava kontrole pristupa. Štoviše, oni su u većini slučajeva jedini dio koji je fizički vidljiv samom korisniku, to jest nositelju kartice. No iako bi se moglo učiniti da je u njima sadržan kompletni sustav, u većini slučajeva oni su samo periferija kontrole pristupa. Najveći dio čitača kartica zapravo ne donosi odluku o tome hoće li se nositelju kartice omogućiti pristup ili ne, već samo prikuplja informacije s kartice i prosljeđuje ih kontrolnom uređaju, koji onda za danu karticu šalje pozitivan ili negativan signal.

Na najnižoj razini nalaze se kartice s bar-kodom. Takvi sustavi primjenjuju se uglavnom za evidenciju ili na mjestima gdje je kontrola pristupa čisto simbolična, budući da je čitanje i dupliciranje takvih kartica vrlo lako.
Najosnovnija klasa sigurnosno prihvatljivih pristupnih kartica jesu kartice s magnetnom trakom koja sadrži određeni skup informacija. Ta se kartica provlači ili umeće u čitač koji potom čita podatke s magnetne trake. Kartice s magnetnom trakom privlačne su zbog svoje niske cijene i jednostavnosti programiranja; s druge strane, podaci na njima uglavnom nisu dobro zaštićeni i lako ih je duplicirati. Magnetne kartice većinom su dobar izbor za kontrolne točke s relativno niskom vrijednosti ili niskim stupnjem potencijalnog rizika.
Bezkontaktni sustavi predstavljaju napredniji stupanj čitača pristupnih kartica. Oni emitiraju RF polje koje je u stanju očitati podatke s kartice bez izravnog kontakta kartice sa čitačem. Na taj se način produljuje vijek trajanja i kartice i čitača jer je uklonjen element zamora materijala. Pripadne kartice mogu biti aktivne (s ugrađenim izvorom energije) ili pasivne. Prilikom implementacije bezkontaktnih sustava nužno je obratiti pažnju na lokaciju čitača, budući da na dobar dio tih sustava negativno utječe blizina metalnih predmeta.
Danas je u upotrebi velik broj različitih sustava pristupnih kartica i čitača; sa sigurnosnog stajališta, najslabija karika prirođena takvoj kontroli pristupa jest sama kartica. Naime, očito je da kontrolni uređaj dopušta prolaz upravo kartici, neovisno o osobi koja tu karticu posjeduje, te ukradena ili izgubljena kartica predstavlja ozbiljnu prijetnju sigurnosti ukoliko se gubitak ne ustanovi na vrijeme da se preko pripadnog programskog paketa ne ukinu prava koja spomenuta kartica posjeduje. Također, na lokacijama gdje je pristupna kartica jedina metoda kontrole pristupa, ne može se kontrolirati točan broj osoba koje su prošle u zaštićeno područje nakon što je kartici odobren pristup.

Biometrijski čitači

Biometrija je pojam koji se, između ostalog, koristi za proučavanje (i uporabu) metoda prepoznavanja ljudskih bića na osnovu jedne ili više jedinstvenih karakteristika, koje mogu biti fizičke (otisak prsta, prepoznavanje lica, prepoznavanje šarenice) ili vezane uz ponašanje (prepoznavanje glasa). Kada se donosi odluka o vrsti karakteristike koja će se koristiti kao sredstvo identifikacije, moraju se uzeti u obzir neki uvjeti. Prvi od njih je univerzalnost, to jest, svaka osoba mora posjedovati tu karakteristiku; potom, koliko je ta karakteristika jedinstvena, odnosno s kojim stupnjem pouzdanosti pomoću nje možemo razlikovati jednu osobu od druge. Nakon toga slijede trajnost osobine (otpornost na promjene tijekom životnog vijeka osobe), jednostavnost implementacije tehnologije čitača, i druge.
Iako su prednosti biometrijskih sustava očite, sa sigurnosnog aspekta moramo razmotriti i potencijalne nedostatke. Kada koristimo tradicionalnije metoda identifikacije pomoću kartica, sigurni smo da će kontrolni uređaj biti u stanju točno očitati podatke na kartici, budući da su oni i zapisani s tom svrhom u vidu. S druge strane, iako su dobro odbrane biometrijske karakteristike u teoriji jedinstvene, točnost njihov očitavanja uvijek predstavlja kompromis između brzine/učinkovitosti/ekonomičnosti i točnosti. Ako je proces prepoznavanja šarenice dovoljno iscrpan, identifikacija će se izvršiti s gotovo savršenim stupnjem pouzdanosti. Ali u većini slučajeva kontrola pristupa mora zadovoljavati i određeni stupanj brzine, odnosno protočnosti, tako da analiza nikada neće moći biti izvršena na razini laboratorijske analize. Također, postoji i problem prilikom podešavanja osjetljivosti čitača. Ako čitač podesimo na veću osjetljivost, povećava se takozvani FRR (False Reject Rate), odnosno broj ljudi kojima će biti zabranjen pristup iako su u kategoriji „poželjnih“ zato jer je kontrolni sustav bio previše zahtjevan, pa je detalje koji su mogli biti posljedica ambijentalne rasvjete ili nekih drugih parametara protumačio kao temelj za diskvalifikaciju. Nasuprot tomu, ako smanjimo osjetljivost čitača, povećava se FAR (False Accept Rate), to jest postoji mogućnost da će

sustav odobriti pristup nekome na listi „nepoželjnih“ zato jer je neke razlike protumačio kao zanemarive. Većina tih grešaka u vrlo je malom postotku, ali ih se neovisno o tome mora uzeti u obzir.
Kao što je to slučaj sa svim sigurnosnim sustavima, i biometrijske kontrole se mogu zaobići, ali taj postupak je daleko zahtjevniji. Ne postoje kartice koje se mogu ukrasti niti sigurnosne šifre koje vlasnik može nepažnjom ostaviti zapisane na svom računalu. Također, moderni biometrijski sustavi imaju implementirane mjere kojima se osigurava provjera da je subjekt biometrijske analize „živi“, odnosno da uzorak koji se podvrgava testiranju nije fotografija oka, snimka glasa ili odrezani prst. Veća zabrinutost javlja se vezano uz povjerljivost samih uzoraka; budući da naš glas ili oko nije nešto što možemo samo tako zamijeniti, postavlja se pitanje što se događa ako uzorci naših biometrijskih osobina padnu u krive ruke. Debate oko tog problema su opsežne, ali još uvijek nisu pretjerano aktualne uzevši u obzir trenutnu ograničenu rasprostranjenost biometrijskih sustava.

Kontrolni uređaji i programski paketi

Kontrolni uređaj obično se nalazi na sigurnom mjestu udaljenom od čitača i donosi odluke o tome hoće li otvoriti vrata ili ne. Također vodi evidenciju o događajima za eventualnu naknadnu analizu, kao i o nasilno otvaranim vratima ili vratima koja su držana otvorena dulje nego je potrebno da prođe jedna osoba. Moderni sustavi u stanju su funkcionirati neovisno neodređeno dugo, a potrebne promjene ili pregled statistike vrši se preko računalnog terminala.
Odabir sustava kontrole pristupa ovisi o više čimbenika, i to ne samo trenutnih, već i budućih, kao što su planirani razvoj poslovanja, potreba za promjenjivom razinom sigurnosti i slično. Iako na tržištu postoji niz specijaliziranih poduzeća koja će se pobrinuti svojim klijentima dati profesionalne preporuke, poznavanje prednosti i nedostataka pojedinih sustava kontrole pristupa uvijek vam može samo koristiti pri odabiru pravog rješenja za vaše potrebe.