09_AUTENTIFIKACIJA - SSO

Od prvih računara do danas zahteva se kontrola pristupa podacima. Moguće je same računare fizički zaštititi i ograničiti im pristup, ili zahtevati identifikaciju korisnika, pa na osnovu toga dozvoliti pristup određenim podacima.

Proces autentifikacije, odnosno provere korisničkog identiteta, veoma je važan element informatičke bezbednosti. Kako autentifikacija predstavlja prvi korak prijave korisnika u sistem, sigurnosni zahtevi koji se pred nju postavljaju prilično su visoki. Osim visokog nivoa sigurnosti, da bi bio upotrebljiv u praksi, proces autentifikacije mora da zadovoljava i brojne druge zahteve (praktičnost, finansijsku isplativost, jednostavnost održavanja i upravljanja...). Kao primer slabe isplativosti mogu se navesti biometrijski uređaji koji, uprkos visokom stepenu sigurnosti koju nude, još uvek nisu šire prihvaćeni kao mehanizam autentifikacije.

U svakodnevnom poslu postoji potreba za čestim prijavljivanjem na više sistema i pri tome se upotrebljavaju različita korisnička imena i autentifikacijske informacije.
Upravo u tom području pomaže uvođenje protokola “autentifikacije i autorizacije korisnika na jednom mestu“ ili “jednostruke autentifikacije“. Taj protokol smanjuje ljudske greške, jer je potrebno pamtiti mnogo manje lozinki, a ujedno I štedi vreme .

JEDNOSTRUKA PRIJAVA

Jednostruka prijava (poznata pod engleskim nazivom **Single Sign-On** – ili skraćeno **SSO**) predstavlja proces autentifikacije koji omogućava korisniku očitavanje ličnih akreditacijskih podataka samo jednom, kako bi korisnik mogao da pristupi različitim resursima (npr. aplikacijama).
Posle autentifikacije korisnik može da izvršava aplikacije za koje je autorizovan. Drugim rečima, SSO predstavlja deljenje autentifikacijskih podataka. Za primer se može uzeti neka firma, tamo gde zaposleni, kako bi izvršavao svoje obveze, mora da ima pristup određenim podacima, u zavisnosti od vrste posla koje obavlja. Očigledno je firmi potreban autentifikacijski mehanizam koji će dodeljivati uloge radnicima, na osnovu kojih se određuju dozvole pristupa podacima. Dakle, firma može imati nekoliko aplikacija kojima se pristupa korišćenjem korisničkog imena i lozinke. Korisnik jedne aplikacije u nekom trenutku želi da koristi drugu aplikaciju. Postavlja se pitanje kako to omogućiti? Postoje dve mogućnosti:

• Imena i lozinke se mogu duplirati i postaviti u bazu na svakoj aplikaciji. Tako pojedina aplikacija posebno proverava validnost imena i lozinke. Očigledno je da postoji redundancija jer se kod pristupa svakoj aplikaciji potrebno ponovo prijaviti.

• Drugi način je bez redundancije. Ako se korisnik prijavi na jednoj aplikaciji, tada se njegovi podaci prosleđuju ostalim aplikacijama. Jedini zahtev je da dve aplikacije međusobno veruju jedna drugoj.

SSO nije bez mana, ali ipak pruža više od problema koji se javljaju, pa se SSO sve više koristi. Uobičajeno je da se SSO modul izdvaja u posebni deo. Otuda i naziv “autentifikacija na jednom mestu“. Sve aplikacije veruju da će taj modul proveriti ime i lozinku korisnika. Korišćenje SSO donosi sledeće prednosti:

• Povećana produktivnost korisnika – omogućeno je da korisnici unose autentifikacijske podatke na samo jednom mestu za sve usluge koje koriste u jednom trenutku.

• Autentifikacija je bazirana na jedinstvenoj bazi sigurnosnih podataka.

• Postoji propagiracija bezbednosnih atributa kroz system.

• Korisnik pamti samo jedno korisničko ime/lozinku za sve aplikacije

• Administratori održavaju centralizovani repozitorijum korisnika za ceo sistem.

• Redukovani troškovi uvođenja i održavanja.

• Jednostavnije razvijanje novih aplikacija - programeri ne brinu o autentifikaciji. Mogu da pretpostave da je korisnik uspešno autentifikovan kada dođe zahtev za aplikacijom i zajedno sa njim i korisničko ime/lozinka.

• Ostvarenje SSO rešenja može da se sprovede u koracima, najpre na jednom delu aplikacija, da bi se onda krenulo na preostali deo.

Problemi koji se javljaju sa SSO rešenjima uključuju sledeće:

• Promena postojećih aplikacija. Ostvarenja SSO rešenja za promenu postojećih aplikacija mogu biti komplikovana, dugotrajna i skupa.

• Računari bez nadzora - ako se korisnik uspešno prijavi na SSO intrefejs, pa se udalji od računara i ostavi ga bez nadzora – ovo je generalno, pitanje bezbednosti, a u SSO slučaju je posebno opasno jer su svi autorizovani resursi kompromitovani.

• Jedna tačka napada - sve aplikacije koriste usluge jednog interfejsa koji je glavna meta zlonamernih napada.