Zakaj in kako: Avtentikacija in avtorizacija - OpenLDAP, Moodle, OpenProject, Linux?

red. prof. dr. Robert Leskovar

Generirano 21/11/2021 ob 21:18:46

Povzetek

Spominčica (memo) razlaga pojma avtentikacija in avtorizacija. Navedeni so primeri uporabe imeniškega strežnika OpenLDAP, učnega okolja Moodle, orodja za vodenje projektov OpenProject in operacijskega sistema Linux.

Kazalo

1 Avtentikacija in avtorizacija

Pri vsakodnevni uporabi spletnih strani, internetnih storitev, oblačnih storitev v povezavi z varnostjo informacijskega sistema, kibernetsko varnostjo, varnostjo osebnih podatkov naletimo na dva pojma, ki se pogosto pojavljata: avtentitkacija in avtorizacija. To nista sopomenki, skoraj vedno pa se pojavljata skupaj.

1.1 Avtentikacija je proces preverjanja istovetnosti

Preverjanje istovetnosti je realizirano na različne načine:

- Najpreprostejši način preverjanja identitete je vnos uporabniškega računa in gesla, ki je določen temu uporabniškemu računu. Sledi primerjava vnesenih podatkov s podatki, ki jih shranjuje oz. do njih dostopa storitev. Če so podatki identični (vneseni račun je enak shranjenemu računu in vneseno geslo je enako shranjenemu geslu), potem ta avtentikacijski mehanizem (to je običajno programski modul) v vmesniku sporoči, da je prepoznava uspela. Če prepoznava ni uspela, se uporabniško ime in geslo ne ujemata. Posledica tega je, da uporabnik storitve oz. rešitve ne more uporabljati. Posamezne rešitve imajo lahko vgrajena pravila za gesla: dolžina (minimalna in maksimalna dolžina), uporaba malih, velikih črk, posebnih znakov, cifer, prepoved, da geslo vsebuje uporabniško ime (ali osebnih imen), pri spreminjanju prepoved uporabe prejšnjih gesel in podobno.
- Če storitev po sprejemu imena in gesla od uporabnika zahteva še npr. odgovor na sporočilo SMS ali kodo QR (to uporabnik vnese v vmesnik s prepisovanjem ali skeniranjem), govorimo o dvofaktorski avtentikaciji. Pri dvofaktorski avtentikaciji se namesto SMS pogosto uporabljajo aplikacije na mobilnih napravah ali pa posebne naprave (običajno velikosti kreditne kartice). Tako mobilne aplikacije kot naprave temeljijo na generatorjih naključnih števil. Če storitev zahteva več kot dva načina preverjanje istovetnosti, gre za večfaktorsko avtentikacijo.
- Pri preverjanju istovetnosti se pogosto uporablja infrastruktura javnih in zasebnih ključev. Javni in zasebni ključ sta običajno veliko daljša (npr. 2048, 4096 znakov) kot prej omenjeno geslo. Ključa sta običajno zapisana v datoteki ali v polju baze podatkov. Storitev ima v tem primeru shranjen samo javni del uporabnikovega ključa, uporabnik pa ima svoj zasebni in javni del ključa. Sporočilo, ki je šifrirano z zasebnim delom ključa, je storitvi razumljivo le, če dešifriranje z javnim delom ključa vrne smiseln odgovor. V praktični uporabi je priporočljivo, da je vsak dostop do zasebnega ključa možen le ob vpisu gesla, ki ga je uporabnik posebej za ta primer predvidel ob generiranju zasebnega in javnega ključa.
- Uporaba zaupanja vredne storitve, ki komunicira s ciljno storitvijo. Zaupanja vredna storitev omogoča preverjanje identitete za poljubno število

želenih storitev. Taka storitev ima kratico SSO (ang. kratica za Single-Sign-On).

- Popularen je še način overjanja istovetnosti s pomočjo platform za družabna omrežja.

V splošnem velja, da večje število identifikacijskih postopkov poveča zanesljivost pri potrditvi istovetnosti, a hkrati zahteva več časa. Obseg preverjanja je potrebno prilagoditi in pri tem upoštevati kontekst uporabe kot so občutljivost in vrednost podatkov, pogostost preverjanja, poraba časa in podobno.

1.2 Avtorizacija je proces dodeljevanja pravic ali pooblastil

Pri avtorizaciji gre za proces dodeljevanja pravic, ki pripadajo določenemu uporabniku. Pravice uporabe storitve, aplikacije ali njegega dela lahko temelji na: uporabnikovi vlogi v podjetju (npr. komercialist, medicinska sestra, študent, generalni direktor), spletnem žetonu z zapisom JSON (Javascript Object Notation), digitalno podpisanih datotekah XML po standardu SAML, standardu OpenID, OAuth in podobno. Povezava uporabnikove identite in njegovih pravic je najpogosteje vgrajena v konkretno storitev oziroma v aplikacijo (npr. Wordpress, Moodle, OpenProject, GitLab), lahko pa so tudi pravice shranjene na enem mestu (avtorizacijska baza, avtorizacijski strežnik).

2 Primeri avtentikacije in avtorizacije

2.1 Avtentikacija in avtorizacija v aplikaciji

Aplikacije kot so npr. Wordpress, Moodle, OpenProject vsebujejo bazo podatkov s shranjenimi uporabniškimi imeni in pripadajočimi gesli. Tabele v bazi podatkov vsebujejo tudi seznam pravic uporabnika. Navedene aplikacije lahko interno izvajajo avtentikacijo in avtorizacijo. Programska rešitev najprej primerja vnesene podatke s podatki v lastni bazi - avtentikacija. Nato primerja uporabnikovo zahtevo (npr. vpogled v seznam objavljenih člankov, sprememba podatkov o študentu, brisanje uporabnika in vseh njegovih projektnih aktivnosti ter rezultatov) ter seznam njegovih pravic. Rezultat primerjave je lahko dovoljenje ali prepoved izvedbe zahteve. Pogosto imajo aplikacije vgrajene še druge module za avtentikacijo z različnimi metodami. Poleg interne avtentikacije so to lahko avtentikacija s strežniki CAS, SSO, IMAP, LDAP, PAM, POP3, Shibboleth in RADIUS.

2.2 Avtentikacija s strežnikom LDAP in avtorizacija v aplikaciji

Za tak primer je potrebno najprej namestiti imeniški strežnik (LDAP). Ena od možnih rešitev je uporaba odprtokodnega imeniškega strežnika OpenLDAP. Za

potrebe pedagoškega procesa smo v Laboratoriju za kakovost in testiranje programske opreme UM FOV izdelali Linux-ov vsebnik (LXC, Linux Container) na naslovu IP [redacted] Definirali smo kontekst:
`DN: cn=[redacted],dc=[redacted],dc=[redacted]dc=[redacted]`. Podrejeni elementi pa so imeli tip `posixAccount`. Masovni uvoz uporabnikov smo izvedli z datoteko csv, ki jo podpira LDAP Account Manager. Primer:

```
dn_suffix,dn_rdn,inetOrgPerson_firstName,
inetOrgPerson_lastName,inetOrgPerson_email,
posixAccount_cn,posixAccount_userName,
posixAccount_uid,
posixAccount_grouposixAccount_additionalGroups,
posixAccount_homedir,
posixAccount_createHomeDir,
posixAccount_shell,posixAccount_password,
posixAccount_passwordDisabled,
posixAccount_gecos,employeeNumber
"cn=[redacted],dc[redacted],dc=[redacted],dc[redacted]",uid,
[redacted],[redacted],[redacted]@student.um.si,
[redacted],[redacted],[redacted],[redacted],
[redacted],
/home[redacted],[redacted],
/bin/bash,{SASL}[redacted],false,
[redacted],[redacted]
```

Novo skupino z že vpisanimi študenti smo kreirali z datoteko csv (v LDAP Account Manager) takole:

```
dn_suffix,dn_rdn,posixGroup_description,
posixGroup_cn,posixGroup_gid,
posixGroup_password,posixGroup_members
"cn=[redacted],dc=[redacted],dc=[redacted]dc=[redacted]",cn,[redacted],
[redacted],[redacted],[redacted]
"[redacted]
```

Kadar so bile v datoteki csv kakšne napake, se uvoz ni izvedel in dobili smo sporočilo. V primeru uspešnega uvoza smo v spletnem vmesniku videli nove uporabnike oz. nove skupine z definiranimi uporabniki.

Uporaba strežnika LDAP v različnih aplikacijah in operacijskih sistemih zahteva specifične prilagoditve:

- Moodle omogoča avtentikacijo z vtičnikom (celotna aplikacija je napisana v jeziku PHP). Ta vtičnik omogoča tudi spreminjanje gesla na imeniškem strežniku, sinhronizacijo računov in mapiranje polj (LDAP:Moodle). Poleg avtentikacije lahko ta vtičnik omogoča avtorizacijo na nivoju uporabniških vlog (npr. manager, course creator) in kreiranje uporabnika v strežniku LDAP.

- OpenProject omogoča le avtentikacijo (celotna aplikacija je napisana v jeziku Ruby). V primerjavi z Moodlovim vtičnikom ima ta vtičnik manj funkcij, saj omogoča le nastavitve kriptiranja, povezovanje s strežnikom LDAP ter mapiranje nekaterih polj (LDAP:OpenProject)
- Linux omogoča avtentikacijo z modulom PAM (Pluggable authentication module). Najprej je na Linux-u potrebno spremeniti nekaj konfiguracijskih datotek, nato pa namestiti knjižnice za strežnik LDAP. Pri namestitvi knjižnic je potrebno vpisati značilnosti imeniškega strežnika (LDAP). Ker je Linux zgrajen kot večuporabniški operacijski sistem, ima lahko le en imeniški strežnik funkcijo storitve SSO.

3 Zaključek

V spominčici so predstavljeni primeri uporabe imeniške storitve LDAP v okolju z veliko uporabniki in različnimi aplikacijami in operacijskimi sistemi. Zapis ne vsebuje občutljivih podatkov o naslovu imeniškega strežnika ter resničnih podatkov v uporabnikih in skupinah. Prav tako niso prikazane detajlne nastavitve apliacij Moodle ter OpenProject in operacijskega sistema Linux. Kogar zanimajo te podrobnosti naj se poduči v specifičnih priročnikih navedenih orodij ([2], [3], [4]).

Literatura

[1] lrshivangini. Authentication vs. Authorization Defined: What's the Difference? [Infographic] June 11, 2020

[2] Moodle 3.9.

[3] Openproject.

[4] Ubuntu.