Infrastruktura javnih ključeva

Bezbednost u sistemima elektronskog plaćanja
Prva kontrolna tačka

Kontekst

MegaTravel je multinacionalna korporacija koja nudi usluge organizacije putovanja mušterijama širom sveta. Kako bi podržala milione mušterija i hiljade zaposlenih, kao i očuvala položaj svetskog lidera na tržištu, MegaTravel raspolaže sa značajnim brojem softverskih podsistema, od internih alata i informacionih sistema, do servisa dostupnih putem interneta. Zbog velike količine vrednih podataka i svoje pozicije na tržištu, softver ove korporacije predstavlja značajnu metu za napad od strane kriminalaca i konkurenata.

Bitan čvor za bezbednost MegaTravel sistema predstavlja podsistem za infrastrukturu javnih ključeva (u daljem tekstu *PKI*). Uz pomoć ovog podsistema, security administrator (u daljem tekstu *admin*) može da poveća bezbednost MegaTravel sistema, tako što:

- Omogućuje autentifikaciju softverskih sistema;
- Pruža podršku za kontrolu pristupa između softverskih sistema;
- Štiti poverljivost i integritet poruka koje se razmenjuju između softvera i ljudi, putem šifrovane komunikacije.

Cilj zadatka

Kao glavni rezultat ovog zadatka, svaki student treba da stekne jasnu sliku koju ulogu sertifikati i PKI podsistem igraju u distribuiranom softverskom sistemu, kako se integrišu sa istim, i koje komplikacije i problemi postoje u ovoj priči.

Specifikacija

Specifikacija zadatka je definisana kroz niz obimnih korisničkih priča, formiranih od strane admina. Za svaku priču, navedeno je nekoliko teza kako bi se istakli aspekti koji preciznije definišu zadatak i ovo treba uzeti u obzir pored samog teksta korisničke priče. Potrebno je dizajnirati i implementirati PKI vođeni ovim zahtevima.

Napomena: Na vežbama je diskutovan inicijalni dizajn PKI podsistema. Nije obavezno da se u potpunosti pridržavate definisanog dizajna, već se i očekuje da će se on nekoj meri menjati kako budete radili na vašem rešenju.

As a security administrator,
I want to centrally issue certificates for my system's software,
So that I can easily manage the digital identities of software in my system.

- Adminu treba omogućiti da izda bilo koji sertifikat u lancu sertifikata.
- Admin treba da ima uvid u sertifikate koji postoje na sistemu.
- PKI treba da uzme u obzir validnost sertifikata u kontekstu izbora izdavaoca.
- Admin treba što više olakšati popunjavanje svih podataka koji su potrebni za sertifikat.
- Obratiti pažnju na *best practice* konfiguraciju bezbednosnih funkcija koje koristite.
- Potrebno je pripremiti nekoliko smislenih sertifikata za kontekst MegaTravel preduzeća.

As a security administrator,
I want to revoke certificates when the need arises,
So that I can maintain the integrity of my PKI.

- PKI treba da pruži servis za proveru da li je sertifikat povučen.

As a security administrator,
I want to control which applications can communicate with each other,
So that I can prevent threat agents from harming my system.

- Ako app A može da komunicira sa app B, app B može da komunicira sa app A.
- PKI može, ali ne mora samostalno da rešava ovaj zahtev, no treba što više da podrži admina i da tim ima jasnu sliku kako se rešava deo koji PKI ne rešava.

As a security administrator,
I want to securely distribute digital certificates to the different software,
So that I can efficiently replace and install certificates across the system.

- PKI može, ali ne mora samostalno da rešava ovaj zahtev, no treba što više da podrži admina i da tim ima jasnu sliku kako se rešava deo koji PKI ne rešava.
- Obratite pažnju na zahtev da distribuiranje bude bezbedno i efikasno.
- Na odbrani, tim treba da ima jasnu sliku koji su koraci koje će admin da radi prilikom inicijalne instalacije sertifikata (npr. kada se sistem proširi novim softverom), kao i šta će se dešavati kada je potrebno zameniti istekli sertifikat.