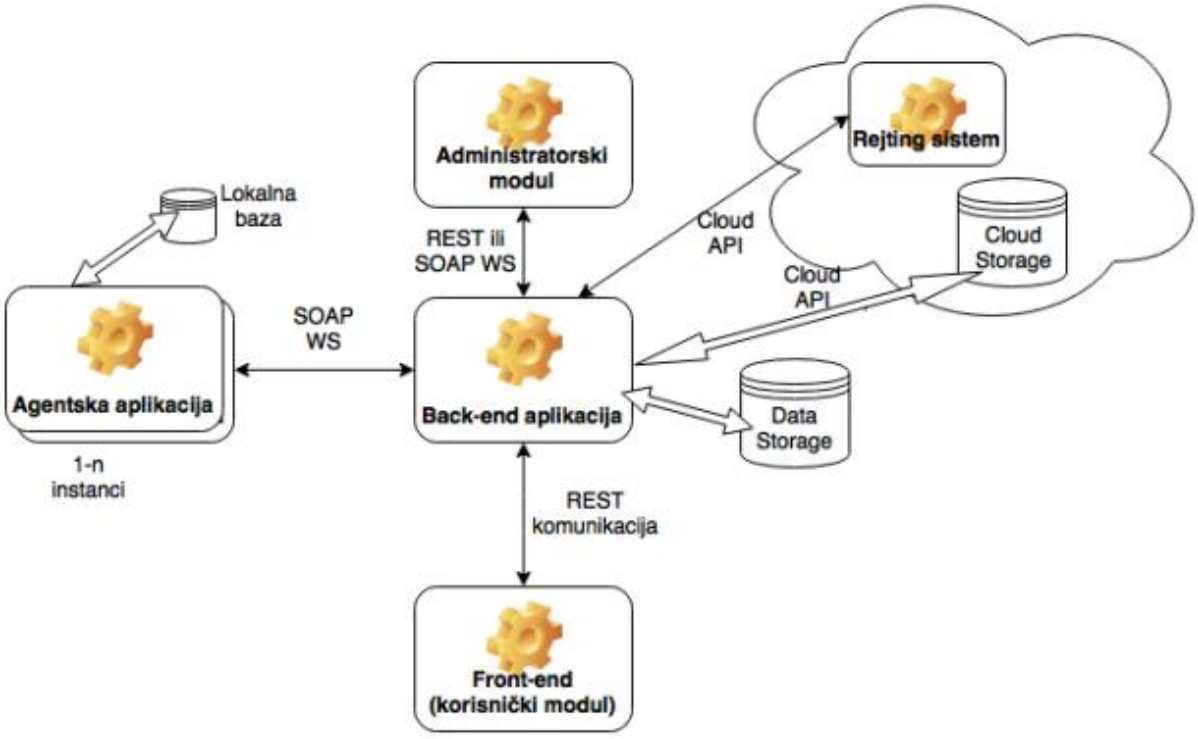
OBEZBEĐIVANJE SISTEMA ZA UPRAVLJANJE I RENTIRANJE SMEŠTAJA

Bezbednost u sistemima elektronskog poslovanja
Verzija 1
2018.

1. PREGLED SISTEMA

U okviru projektnog zadatka iz predmeta Bezbednost u sistemima elektronskog poslovanja potrebno je definisati i implementirati bezbednosne mehanizme za zaštitu sistema (Slika 1) definisanog kroz projektni zadatak predmeta XML i web servisi (XWS).



SLIKA 1 PREGLED SISTEMA ZA UPRAVLJANJE I RENTIRANJE SMEŠTAJA

2. STAVKE SPECIFIKACIJE

U ovom poglavlju su definisani podsistemi, dokumenti i bezbednosni mehanizmi koji trebaju da budu implementirani u sklopu projekta. Tehnologija koja se koristi za realizaciju tačaka specifikacije je proizvoljna.

2.1 PODSISTEM ZA UPRAVLJANJE KLJUČEVIMA

Napraviti veb-aplikaciju za PKI koja podržava sledeću funkcionalnost:

1. Generisanja samopotpisanih sertifikata za sertifikaciona tela. Korisnik putem forme unosi podatke potrebne za sertifikat, nakon čega se generiše sertifikat (koji sadrži javni ključ), i privatni ključ,

uskladišten u Java KeyStore (ili prikladno skladište za relevantnu tehnologiju). Generisan sertifikat se može koristiti za potpisivanje drugih sertifikata;

2. Generisanje sertifikata za sertifikaciona tela. Funkcionalnost slična kao prethodna, gde korisnik pored relevantnih podataka navodi i sertifikat koji će potpisati nov sertifikat. Sertifikat se bira iz liste prethodno generisanih sertifikata koji nisu istekli niti su povučeni. Za izdavanje sertifikata mogu se koristiti samo sertifikati sa CA = true atributom. Generisan sertifikat se može koristiti za potpisivanje drugih sertifikata;
3. Generisanje sertifikata krajnjih korisnika (pravnih lica). Funkcionalnost slična kao prethodna, gde generisan sertifikat ne može da se koristi za potpisivanje drugih sertifikata;
4. Preuzimanje postojećih sertifikata. Korisnik prosleđuje serijski broj sertifikata i dobija sertifikat;
5. Povlačenje sertifikata. Korisnik prosleđuje serijski broj sertifikata, nakon čega sistem povlači sertifikat;
6. Provera da li je sertifikat povučen po uzoru na OCSP protokol. Korisnik prosleđuje serijski broj sertifikata i dobija njegovo stanje.

Sertifikati su formirani po X.509v3 standardu. Iskoristiti ovu aplikaciju da se konstruiše stablo sertifikata za čitavo informatičko postrojenje koje se razvija u sklopu XWS projekta. Za svaki sertifikat, pored osnovnih informacija o vlasniku i trajanju sertifikata, treba da bude definisano AIA i CDP polje, kao i polje za identifikaciju svrhe sertifikata.

BONUS

Osmisliti prikladan sistem kontrole pristupa, tako da:

- Funkcionalnostima 1., 2. i 5. može pristupiti administrator sistema;
- Funkcionalnost pod 3. se izvršava tako što vlasnik sertifikata pravi CSR dokument koji šalje CA-u koji potom generiše sertifikat;
- Funkcionalnostima 4. i 6. može bilo ko da pristupi.

2.2 MODEL PRETNJI

Napraviti model pretnji sistema za upravljanje i rentiranje smeštaja. Model treba da uključi:

- Dekomponovanje sistema sa identifikovanim resursima, nivoima poverenja, pretpostavkama, itd.;
- Dijagram toka podataka koji identifikuje celine sistema;
- Spisak identifikovanih resursa i pretnji uz opis napada koji realizuju pretnje;
- Reprezentativna stabla napada (imaju bar tri načina napada) za bar dve pretnje visoke kritičnosti;
- Sračunate rizike i određene strategije regulisanja rizika.

2.3 ZAŠTITA PODATAKA

Osetljivi podaci sa kojim aplikacija radi treba da budu obezbeđeni u skladištu, u transportu i tokom upotrebe. Putem modela pretnji identifikovati osetljive podatke, nakon čega treba definisati i implementirati prikladne bezbednosne kontrole.

Podaci čije skladištenje se ne može izbeći treba da budu šifrovani ili heširani ukoliko je to prikladno.

XML dokumenti koji se razmenjuju putem SOAP protokola treba da budu digitalno potpisani i šifrovani upotrebom implementacije XML Signature & Encryption standarda, gde komunikacija treba dodatno da bude zaštićena od reply napada.

Komunikacija između veb-čitača i servera treba da bude zaštićena sigurnom konfiguracijom HTTPS protokola.

2.4 UPRAVLJANJE KORISNICIMA

Informacioni sistem treba da podrži prikladne mehanizme za autentifikaciju i autorizaciju.

Mehanizmi autentifikacije treba da podrže bezbednu registraciju, prijavu na sistem, odjavu, promenu lozinke i resetovanje lozinke. U slučaju korisničkih naloga zaposlenih, funkcije registracije i resetovanja lozinke ne treba implementirati, te ove korisnike instalirati upotrebom SQL skripti.

Autorizacija podrazumeva kontrolu pristupa po RBAC modelu, gde različite role treba definisane za konkretni informacioni sistem. Implementirati mehanizam koji će omogućiti kontrolu pristupa nad distribuiranim sistemom, koji uključuje jednu ili više agentskih aplikacija i centralnu aplikaciju (Slika 1).

2.5 Bezbednost u razvoju softvera

Prilikom razvoja softverskog rešenja treba voditi računa o adekvatnoj organizaciji i implementaciji bezbednosnih mehanizama za validaciju podataka, autentifikaciju, autorizaciju, i logovanje. Logovi treba da sadrže relevantne podatke i da imaju ispravnu strukturu. Tokom implementacije pratiti bezbednosne principe poput višeslojne odbrane, najmanje privilegije, bezbednog otkaza, itd.

Potrebno je uraditi gap analizu između implementiranog sistema i OWASP Top 10 rizika i formirati izveštaj gde se objašnjava koje grupe napada su relevantne, i kako je sistem zaštićen od njih, ili kako bi bio zaštićen prilikom postavljanja u produkciju.

Bonus

Uraditi gap analizu između implementiranog sistema i OWASP ASVS standarda.

Bonus

Sprovesti penetraciono testiranje veb-aplikacija i servera upotrebom bar dva alata iz grupe: Nmap, Nikto, dirbuster, sqlmap, OWASP ZAP, Burp Suite. Formirati izveštaja penetracionog testa i regulisati slabosti.

Napomena

Za ocenu 10 je neophodno uraditi makar jednu Bonus stavku. Dalje, stavku specifikacije je moguće zameniti sa nekim bonus zadatkom, sa ograničenjem da je neophodno da se uradi stavka kojoj bonus pripada. Studenti su ohrabreni da se bave stvarima koje su im interesantne u kontekstu bezbednosti softvera.