Kućni sigurnosni sistem

Bezbednost u sistemima elektronskog poslovanja

2021/2022

I Uvod

Kućni sigurnosni sistem je sistem koji se koristi za obezbeđivanje imovine, bilo da se radi o stanu, vikendici ili kući (u daljem tekstu objekat). Uz pomoć ovog sistema, može da se prati da li se nešto nepredviđeno desilo, kao što je nestanak struje, nasilno otvaranje vrata i prozora, pomeranje elemenata u objektu itd. Sistem je veoma lak za upotrebu i rukovanje. Sva upozorenja i obaveštenja su razumljiva i intuitivna za korisnika.

Kućni sigurnosni sistem se sastoji od velikog broja softverskih podsistema, različitih internih alata i informacionih sistema, kao što su *Moja kuća, Admin aplikacija* i različiti *uređaji*.

Aplikacija *Moja kuća* služi za bežičnu kontrolu, monitoring i upravljanje sistemom jednog objekta.

Promene, u okviru jednog objekta, generišu različiti *uređaji* kao što su: kamere, alarmi, uređaji za praćenje rasvete, uređaji za otvaranje kapija, brava..

Admin aplikacija se koristi za konfiguraciju sistema i očuvanje bezbednosti.

Sistem raspolaže sa velikom količinom osetljivih podataka, te predstavlja metu za različite vrste napada. Potrebno je obezbediti ceo sistem, tako da osetljivi podaci ne dođu u posed napadača.

II Admin aplikacija

Admin aplikacija je bitna za očuvanje bezbednosti čitavog sistema. Funkcionalnosti ove aplikacija se mogu podeliti u 3 dela. Jedan deo funkcionalnosti predstavlja podršku infrastrukture javnih ključeva (PKI), drugi deo služi za konfigurisanje korisnika u sistemu, a treći deo za konfiguraciju aplikacije *Moja kuća* i uređaja koji se prate.

Ovu aplikaciju može da koristi samo super admin i uz pomoć nje da izvršava sledeće funkcionalnosti:

I. **Infrastruktura javnih ključeva**
   A. Centralizovano kreiranje sertifikata

      Prilikom kreiranja sertifikata, aplikacija treba super adminu da što više olakša popunjavanje podataka, koji su potrebni za sertifikat.

      Omogućiti templejte za sertifikate, gde se templejtom definišu ekstenzije koje će ući u sertifikat, a pre svega namena sertifikata.

   B. Povlačenje sertifikata
   C. Uvid u sertifikate

      Za svaki sertifikat treba da bude prikazano da li je validan ili ne, što znači da aplikacija treba da sadrži servis za proveru da li je sertifikat validan.

   D. Distribuiranje sertifikata

      Super admin može da distribuira sertifikate, te je potrebno osmisliti korake koje će super admin izvršavati. Aplikacija treba da ga podrži prilikom tog procesa, tako da sertifikat bude bezbedno i efikasno instaliran.

II. **Korisnici sistema**
   A. Dodavanje korisnika
   B. Menjanje uloge korisnika u sistemu
   C. Brisanje korisnika iz sistema
   D. Pregled svih korisnika (pretraga, filtriranje)

III. **Konfiguracija *Moje kuće* i uređaja**
   A. Definisanje i povezivanje uređaja sa aplikacijom *Moja kuća*

      Moja kuća ima konfiguracioni fajl, koji sadrži spisak uređaja koji se prate. Super admin treba da, za svaki uređaj, koji se prati, definiše: putanju, period čitanja poruka i filter u vidu regexa.

   B. Prikaz svih logova koje su generisale aplikacije

C. Pretraga logova po različitim poljima, sa mogućnošću upotrebe regularnih izraza
D. Pregled alarma
E. Kreiranje pravila za okidanje alarma

Super admin ima zadatak da prati da li je neko pokušao da izvrši napad na neku od aplikacija u sistemu.

Sve aplikacije inicijalno treba da poseduju više pravila, kao što su npr:

- Neuspešni pokušaji prijave na sistem sa istim korisničkim imenom
- Pojava loga čiji tip je ERROR
- Pojava loga u kom se nalazi IP adresa sa spiska malicioznih IP adresa
- Detekcija suviše učestalih zahteva itd..

Osim inicijalnih pravila, super admin može sam da kreira i doda novo pravilo. Pravilo za okidanje alarma se kreira kombinacijom različitih parametara. Pravilo može da se primenjuje na sve aplikacije ili samo na određenu aplikaciju, jer aplikacije neće pratiti iste tipove uređaja npr. jedan objekat može da ima kamere, a drugi da ih nema.

U sklopu admin aplikacije potrebno je kreirati i jednu stranicu kojoj mogu svi da pristupe. Na toj stranici novi korisnici mogu da podnesu zahtev za instalaciju aplikacija i ujedno da pošalju zahtev za potpisivanje sertifikata (CSR). Nakon što korisnik podnese zahtev, super admin treba da ga odobri, generiše odgovarajuće sertifikate i distribuira ih.

III Moja kuća

Moja kuća predstavlja softver koji prikuplja, normalizuje i filtrira događaje, kako bi detektovao i alarmirao korisnike o promenama. Ova aplikacija vrši svoj posao centralizovanim skupljanjem i analizom poruka, koje prima od *uređaja*. Upotrebom sistema zasnovanim na pravilima, ovaj alat korelira događaje koji se dešavaju u nekom vremenskom periodu i na osnovu njih odlučuje da li će okinuti nekakav alarm i upozoriti korisnika na nepredviđeno dešavanje.

Funkcionalnosti koje su dostupne korisnicima ove aplikacije su:

A. Pregled svih uređaja
B. Prikaz svih poruka
C. Filtriranje poruka
D. Generisanje izveštaja bitnih aktivnosti u određenom vremenskom periodu

Potrebno je podržati situacije kada korisnik poseduje više objekata (nekretnina) koji se obezbeđuju i kada postoji više korisnika koji mogu da prate samo podskup tih objekata.

IV Uređaji

Uređaj predstavlja aplikaciju koja prati različite signale iz okruženja. Svaki uređaj, u skladu sa svojom namenom, prati određenu vrstu promena (više neuspešnih pokušaja otvaranja vrata, paljenje/gašenje svetla, promena temperature, pojava nepoznatnog objekta, isključivanje uređaja, prekid komunikacije itd). Uređaji treba da generišu poruke u standardizovanom formatu, da ih dopune bitnim informacijama i proslede aplikaciji *Moja kuća*.

Pored generisanja različitih stanja uređaja, treba kreirati i skriptu, koja će funkcionisati kao state mašina, tj. simulirati normalno stanje i stanje napada. U stanjima normalnog rada, treba da se generišu događaji koji su relevantni za kreirane alarme, ali ih ne okidaju. U stanjima napada treba da se generišu događaji koji će okinuti neki od kreiranih alarma. Potrebno je definisati više stanja za normalan rad i za napade.

V Nefunkcionalni zahtevi

1. Tehnologije

Tehnologije koje se koriste za implementaciju bilo koje celine ovog sistema su proizvoljne.

Obavezno je korišćenje Sistema za kontrolu verzija git. Kao udaljeni repoziorijum, može se koristiti *Github* ili *Gitlab*. Neophodno je da projekat bude u privatnom repozitorijumu, na koji će profil *bezbednost-ftn* biti dodat kao collaborator/reporter.

Komponente za alarmiranje treba da budu bazirana na ECA (Event Condition Action) pravilima, tj. da se za implementaciju koristi Rule-based sistem.

Logovi treba da se čuvaju u noSQL bazi.

Prilikom implementacije svih aplikacija potrebno je konfigurisati bezbednosne funkcije u skladu sa preporučenim, najboljim praksama.

2. Bezbednost resursa

Osetljivi podaci sa kojim aplikacija radi treba da budu obezbeđeni u skladištu, u transportu i tokom upotrebe. Identifikovati osetljive podatke i definisati i implementirati prikladne bezbednosne kontrole. Podaci, čije skladištenje se ne može izbeći, treba da budu šifrovani ili heširani, ukoliko je to prikladno.

Komunikacija između veb-čitača i servera treba da bude zaštićena sigurnom konfiguracijom HTTPS protokola. Sertifikate generisati putem admin aplikacije.

Poruke koje se razmenjuju treba da budu digitalno potpisane od strane uređaja koji ih šalju.

3. Upravljanje korisnicima

Korisnički interfejs alata treba da podrži prikladne mehanizme za autentifikaciju i autorizaciju. Autorizacija podrazumeva kontrolu pristupa po RBAC modelu.

Sistem sa svim svojim *endpoint*-ima treba da ima regulisane sve rizike sa aktuelne OWASP Top 10 liste.

VI Zadaci za ocenu 10

Za ocenu 10 potrebno je uraditi jedan od dva dodatna zadatka *Penetration testing* ili *Secure deployment and disposal.*

Penetration testing

Sprovesti penetraciono testiranje veb-aplikacija i servera upotrebom bar dva alata iz grupe: *Nmap, Nikto, dirbuster, sqlmap, OWASP ZAP, Burp Suite*. Penetraciono testiranje je tehnika za testiranje sigurnosti sistema simuliranjem napada, gde se na osnovu rezultata može izvršiti procena sigurnosti sistema. Potrebno je formirati izveštaje penetracionog testa i regulisati ranjivosti. Kroz ovaj zadatak, studenti će naučiti osnove „hakovanja“, odnosno specijalizovanog testiranja uz pomoć alata, čija svrha je identifikacija ranjivosti u softverskom sistemu.

Secure deployment and disposal

Potrebno je izučiti system hardening i secure disposal procedure i najbolje prakse, i definisati protokol kako će se sistem postaviti u produkciju i kako će se bezbedno ukloniti kada dođe end-of-life sistema. Kroz ovaj zadatak, studenti će naučiti šta podrazumeva postavka sistema u produkciju, kako se obezbeđuje infrastruktura (hardware, OS, serveri) na koje softver leže, i o čemu sve treba voditi računa kada se softver vadi iz produkcije.

Kontrolna tačka 1

Za prvu kontrolnu tačku potrebno je implementirati PKI (infrastruktura javnih ključeva) tj. prvi deo funkcionalnosti admin aplikacije:

- slanje i obrada CSR,
- centralizovano kreiranje sertifikata,
- povlačenje sertifikata,
- uvid u sertifikate (pregled sertifikata),
- provera validnosti sertifikata i
- distribuiranje sertifikata.

Raspodela (distribucija) sertifikata ne mora da bude u potpunosti implementirana. Za KT1 je dovoljno da tim osmisli mehanizam kako bi ovaj zahtev realizovao.

Prva kontrolna tačka nosi 8 bodova.

Rok za poslednji commit je 18.04.2022. u 20:00h.

Kontrolna tačka 2

Za drugu kontrolnu tačku potrebno je implementirati autentifikaciju i autorizaciju, drugi deo funkcionalnosti admin aplikacije (rad sa korisnicima sistema) i omogućiti zaštitu od SQL Injection i XSS napada.

Autentifikacija (5)

- Zaključavanje naloga nakon određenog broja neuspešnih prijava (1)
- Polisa za lozinku (dužina lozinke, veliko, malo slovo, znak) (0.5)
- Heširanje lozinke (1)
- JWT token
    - Trajanje tokena (0.5)
    - Verifikacija tokena - provera da je očekivani algoritam postavljen (0.5)
    - Zaštita od krađe tokena (jwt + cookie) (1)
    - Mehanizam da proglasimo token da je nevalidan (0.5)

Autorizacija (2)
Potpun RBAC sa ulogama i permisijama (2)

Validacija podataka (2)
Zaštita od XSS, SQL Injection, validacija podataka i na klijentskoj i na serverskoj strani

Rad sa korisnicima (4)
Dodavanje korisnika i postavljanje objekata (nekretnina) koje mogu da vide, promena uloge korisnika, brisanje i pregled

Druga kontrolna tačka nosi 13 bodova.
Rok za poslednji commit je 23.05.2022. u 23:59h.

Odbrana projekta

Odbrana projekata će biti **od 30. juna do 2. jula**, a satnica će biti objavljena nekoliko dana ranije u okviru ovog dokumenta: Timovi i satnice

Rok za poslednji *commit* je **29.06.2022. u 20:00h**. Svi timovi koji ranije završe projekat mogu i ranije da brane, potrebno je samo da mi se jave da se dogovorimo za tačan datum i vreme.

Pitanja i odgovori

Zamolila bih vas da napišete broj vašeg tima kada šaljete pitanja.

1. **Pitanje:** Da li je potrebno da Certificate Authority i RegistrationAuthority budu dve zasebne aplikacije, ili da ih objedinimo u okviru admin aplikacije.

   Odgovor: Možete sve da objedinite u okviru admin aplikacije.

2. **Pitanje:** Da li u sistemu može biti više admina, ako ima, jel svako od koristi isti rootCA za izdavanje sertifikata ili ima svoj intermediate certificate?

   Odgovor: Možete da osmislite taj deo kako želite. U redu je da i imate jednog admina, jedan rootCA i jedan intermediate i da onda samo generiše leaf sertifikate.

3. **Pitanje:** Da li korisniku dati opciju da izabere da mu sertifikat bude CA s obzirom da mu to nikad neće biti dozvoljeno?

   Odgovor: Ne morate korisniku da dajete opciju da odabere da mu sertifikat bude CA.

4. **Pitanje:** Da li korisnik može prilikom kreiranja zahtjeva za sertifikat da bira algoritam ključa koji će biti korišćen zajedno sa dužinom ključa, režimom rada... ili da to bude zakucano u kodu na najbolju trenutnu praksu?

   Odgovor: Možete korisniku da ponudite da bira dužinu ključa. Ubacite par predefinisanih opcija i inicijalno označite najbolju opciju. Ostalo ne morate da nudite.

5. **Pitanje:** Za authority key identifier i subject alternative name, da li se to u kodu generiše programski (korisnik samo navede da želi tu ekstenziju) ili korisnik prilikom kreiranja unosi sve potrebne podatke kao i u keystore explorer alatu (authority cert serial number, authority cert issuer(general name type/value)...)?

   Odgovor: Korisnik neće unositi dodatne podatke type/value.

6. **Pitanje:** Imam pitanje vezano za templejte i ekstenzije sertifikata. Šta se podrazumjeva pod tim, da li moramo da pokrijemo sve ekstenzije kao u keystore exploreru, pošto ih ima dosta? I da li možemo napraviti par templejta i da admin može da bira između tih ili da dozvolimo adminu pravljenje templejta i čuvanje istih?

   Odgovor: Ne morate da implementirate kreiranje templejta i čuvanje istih. Dovoljno je da ponudite templejte koje i Keystore Explorer nudi. Omogućite

adminu da sam može da dodaje/briše ekstenzije, koje su označene nakon što je izabran templejt.

7. **Pitanje:** Zanima nas gde se kreiraju javni i privatni ključ prilikom kreiranja zahteva za sertifikat (CSR), tj. da li treba da ih kreira aplikant, pa da u zahtevu prosledi samo svoj javni a privatni sačuva, ili treba da ih generiše adminska aplikacija i da na neki način privatni ključ vrati korisniku (mailom ili nekim requestom)?

   Odgovor: Najbolja praksa je da se privatni ključ generiše sa CSR na serveru gde će taj sertifikat kasnije biti i instaliran. Nekad se oslanjamo na eksterne alate koji generišu CSR, pa samim tim i par ključeva. Zato i imamo keystore-ove (specijalni fajlovi) koji mogu bezbedno da čuvaju par ključeva. Što se naše aplikacije tiče, možete sve da generišete u okviru adminske aplikacije. Takođe, možete da ponudite i opciju da korisnik unese već kreirani CSR.

   U redu je da podržite obe opcije ili samo jednu od te dve (korisnik unosi kreirani CSR i/ili CSR se generiše u okviru adminske aplikacije).

8. **Pitanje:** Ko sve ima mogućnost slanja zahtjeva, da li samo registrovani korisnici ili i neregistrovani (u ovom slučaju prilikom odobrenja CSR se i kreira korisnik)?

   Odgovor: Sami možete da odlučite da li će korisnici na početku biti registrovani ili ne.

9. **Pitanje:** Da li je ova funkcionalnost slanja zahtjeva (CSR) vezana za adminsku aplikaciju ili moja-kuća aplikaciju?

   Odgovor: Ovu funkcionalnost implementirajte u okviru adminske aplikacije.

10. **Pitanje:** Šta je najbolja praksa za čuvanje zahtjeva, u fajlu, bazi ili keystoru (mada za ovo nisam siguran da može).

    Odgovor: CSR ne sadrži nikakvu posebnu tajnu, tako da ne morate previše da brinete oko njegovog skladištenja. Kada se kreira sertifikat, CSR nema neki poseban značaj. Naravno, ne morate CSR svima da prikažete. Svako će moći da vidi šta radite, na osnovu podataka koji su uneti u sam CSR, a nema potrebe za tim.

11. **Pitanje:** Kada kreiramo sertifikat, da li se onda fizički brišu CSR fajlovi?

    Odgovor: Možete da obrišete CSR fajl, jer kada se kreira sertifikat on nema neki poseban značaj, ne sadrži nikakvu posebnu tajnu.

12. **Pitanje:** Obavezna polja koja smo pronašli za CSR fajlove su: email, commonName, organization, organizationUnit, city, state, country. Da li su nam svi oni potrebni za projekat?

Odgovor: Da, potrebna su vam sva ta polja. Za organization unit možete da stavite npr. IT, IT Services, IT department...

13. **Pitanje:** Kada se kreira keystore, da li da omogućimo adminu da ga kreira, ili da mi samo napravimo keystore po nekom defaultnom nazivu i šifri kada se pokrene aplikacija?

    Odgovor: Ne morate keystore programski da kreirate. Slobodno generišite keystore pre pokretanja aplikacije.

14. **Pitanje:** Šta znači povlačenje sertifikata?

    Odgovor: To znači da treba da omogućiti povlačenje sertifikata od strane admina, tj. da implementirate OCSP.

15. **Pitanje:** Šta treba da čuvamo u bazi admin aplikacije? Da li sertifikati treba da se čuvaju u bazi ili u java keystore-u?

    Odgovor: Studentima je prepušteno da sami osmisle šta će čuvati u bazi admin aplikacije. Same sertifikate čuvate u keystore-u, a ako vam je potrebno, neke podatke možete da čuvate i u bazi admin aplikacije.

16. **Pitanje:** Ukoliko korisnik izabere ekstenziju authority key identifier, ona će uvijek imati istu vrijednost s obzirom na to da imamo jedan root i jedan intermediate CA. Da li možemo da onemogućimo to?

    Odgovor: To je nešto što će admin da odabere. Ako imate samo 1 root i 1 intermediate onda će admin imati ponuđenu samo tu jednu opciju. Ako u sistem dodate više interCA onda admin treba da dobije više ponuđenih opcija. Pretpostavite da kupac nema veliko domensko znanje. Kupac će znati npr. da odabere za šta mu treba sertifikat (sertifikat za male online prodavnice, sertifikat za neograničen broj poddomena..) i slično.

    Sve detalje vezane za ekstenzije bira administrator, u skladu sa tim šta mu je korisnik tražio, gde admin ima potpunu kontrolu da li će i šta od ekstenzija ući u sertifikat.

17. **Pitanje:** Primer za ekstenzije i templejte

    Odgovor: Primer templejta i ekstenzija možete videti u okviru KeyStore Explorer-a. Koraci:

    - Create a new KeyStore
    - Biramo JKS
    - Generate Key Pair
    - Kliknemo na dugme Add Extensions
    - Kliknemo na dugme Use Standard Template i tu možemo da vidimo primer 4 šablona (templejta)
    - Odaberemo npr. CA

- Otvorite npr. Key Usage i videćete primere ekstenzija za taj šablon
- Kada otvorite Basic Constraints videćete da je označeno Subject is a CA

18. **Pitanje:** Da li formi za unos CSR ima pristup samo admin?

    Odgovor: Formi za kreiranje CSR nema pristup samo admin. Pogledati pitanje 8.

19. **Pitanje:** Ako kljuceve generise admin aplikacija, kako da ona vrati privatni kljuc entitetu kome je potpisala sertifikat?

    Odgovor: Studentima je prepušteno da sami osmisle taj deo (ovo je pitanje distribucije).

20. **Pitanje:** Da li umesto forme za CSR moze da se uploaduje .csr fajl?

    Odgovor: Da, pogledajte pitanje 7.

21. **Pitanje:** U specifikaciji je navedeno da je svaki uredjaj zasebna aplikacija, da li to znaci da je svaki uredjaj server sam za sebe, odnosno da li za svaki uredjaj treba da se na primer napravi po jedan spring projekat?

    Odgovor: Ne morate za svaki uređaj da pravite po jedan Spring projekat. Možete taj deo da rešite na više načina. Možete u jednom projektu sve da obuhvatite, možete da napišete različite skripte, da koristite neki eksterni alat itd.

22. **Pitanje:** Da li je samo admin CA?

    Odgovor: Da, ali možete i da omogućite da se u okviru adminske aplikacije prave i drugi CA. Pravljenje drugih CA ne mora da inicira korisnik, već admin može sam to da napravi. U tom slučaju, admin kada kreira sertifikat može da izabere ko će biti CA (ponudi mu se lista CA koji postoje i on izabere koji želi).

23. **Pitanje:** "Super admin treba da, za svaki uređaj, koji se prati, definiše: putanju, ...". Sta tacno predstavlja putanja?

    Odgovor: Sami osmisliti na koji način će se povezivati moja kuća sa uređajima. Ne mora da bude putanja, već može da bude i neki ID uređaja ili slično.

24. **Pitanje:** Na kojoj relaciji treba da zastitimo komunikacije? Uredjaj - Moja kuca, Korisnik - moja kuca ili nesto trece?

    Odgovor: Na svim relacijama treba da zaštitite komunikaciju.

25. **Pitanje:** Što se OCSPa tiče, da li mi treba da ga implementiramo po RFC6960 ili njegovu modifikaciju kao što je OCSP Stapling ili je jedino bitno da povlačenje ne implementiramo neoptimalno time što ćemo imati listu nevalidnih sertifikata koju klijent mora da povlači?

Odgovor: Bitno je samo da bude optimalno. Možete da koristite neko gotovo rešenje ili da sami implementirate neko optimalno rešenje. Implementacija može da bude jednostavna, ne morate previše da komplikujete ovde.

26. **Pitanje:** Da li možemo koristiti MongoDB bazu?

    Odgovor: Da, možete sve tu da čuvate.

27. **Pitanje:** Šta znači da je ekstenzija *critical*?

    Odgovor: Ako sistem ne može da obradi informaciju iz ekstenzije, koja je critical, on će odbiti sertifikat, jer je ta ekstenzija označena kao bitna.

28. **Pitanje:** Biblioteke za python koje mogu biti od koristi?

    Odgovor: certifi, pyjks, PyJWT, OpenSSL

29. **Pitanje:** Da li kada se povlači sertifikat treba da se unese i razlog povlačenja?

    Odgovor: Da, omogućite da se unese i razlog povlačenja sertifikata. Možete da ponudite par najčešćih razloga i da omogućite ako treba da se unese neki drugi razlog (koji nije ponudjen).

30. **Pitanje:** Da li se KT1 brani na fakultetu ili online?

    Odgovor: Na fakultetu. Sutra (17.04) ću postaviti tabelu sa terminima.

31. **Pitanje:** Da li korisniku treba omogućiti preko frontenda da zahteva povlačenje sertifikata koji će administrator da odobri/odbije (omogućili bismo mu da može i direktno bez zahteva da radi povlačenje) ili je dovoljno da samo administrator može direktno povući a korisniku ako treba povlačenje obraća se na telefon/email

    Odgovor: Nije obavezno da se dodaje na frontend za korisnika, dovoljno je da admin može da povlači sertifikate.

32. **Pitanje:** Da li super admin ima mogućnost da kreira sertifikate nezavisno od CSRa tj. zahteva korisnika?

    Odgovor: Ako želite možete da dodate i tu opciju. Nije obavezno.

33. **Pitanje:** Da li možemo KT1 da branimo kasnije?

    Odgovor: Da, samo mi se javite. Rok za poslednji commit je isti za sve (18.04.2022. u 20:00h).

34. **Pitanje:** Da li je obavezno da se implementira refresh tokena?

    Odgovor: Nije obavezno.

35. **Pitanje:** Koje uloge u sistemu treba da imamo?

    Odgovor: U sistemu treba da imate administratora, koji će upravljati admin aplikacijom. Ostale uloge možete sami da osmislite. Npr. vlasnik (vidi sve nekretnine) i stanar (vidi samo nekretnine koje mu vlasnik/admin dodeli).

36. **Pitanje:** Da li može da postoji više vlasnika tj. da li više korisnika može da vidi sve ili je potrebno da se, u trenutku postavljanja vlasnika, aktuelni vlasnik prebaci na ulogu stanara?

    Odgovor: Možete da imate više vlasnika i više stanara. U trenutku postavljanja nekog stanara za vlasnika, ne morate vlasnika da prebacujete na stanara. Možete da postavite ograničenje da jedan vlasnik ne može drugog da postavi za stanara ili da ubacite još jednu ulogu koja će u hijerarhiji biti iznad vlasnika.

37. **Pitanje:** Na koji način treba da se implementira dodeljivanje objekata (nekretnina) koje može neko da vidi?

    Odgovor: Za RBAC je potrebno da implementirate role i permisije, a deo sa dodeljivanjem objekata možete proizvoljno da izmodelujte.

38. **Pitanje:** Da li Moja kuća može da ima formu za registraciju i da se korisnici tako dodaju u sistem?

    Odgovor: Da, možete na Mojoj kući da imate formu za registraciju i na taj način da omogućite dodavanje novih korisnika, ali morate da povedete računa na koji način ćete povezivati onda objekte sa korisnikom koji se registrovao.

39. **Pitanje:** Da li admin može da se prijavljuje na Moja kuća aplikaciju?

    Odgovor: Da, možete to da omogućite. On je admin, upravlja celim sistemom.

40. **Pitanje:** Da li admin može u okviru Moje kuće da dodaje korisnike, da se cela ta logika dodavanja dešava u okviru Moje kuće ili moramo da omogućimo komunikaciju 2 bekenda?

    Odgovor: Oba pristupa su u redu.

41. **Pitanje:** Da li možemo da imamo samo jednu bazu u sistemu?

    Odgovor: Da.

42. **Pitanje:** Da li možemo da odvojimo autenifikaciju i autorizaciju u odvojeni modul?

    Odgovor: Da.

43. **Pitanje:** Gde možemo da pogledamo primer za RBAC?

    Odgovor: Files > Vežbe > 5. Autentifikacija i autorizacija

44. **Pitanje:** Da li možete da pojasnite tačku "Verifikacija tokena - provera da je očekivani algoritam postavljen"? Da li je to deo validateToken u primeru sa vežbi ili je potrebno nešto dodatno?

    Odgovor: Da, provera da li je očekivani algoritam postavljen je taj deo koji vidite u okviru primera koji sam postavila (vežbe 5).

45. **Pitanje:** Da li je prihvatljivo rešenje povlačenja tokena kreiranje blacklist-e

    Odgovor: Da, to je prihvatljivo rešenje.

46. **Pitanje:** Jedno od pitanja je takođe da li stanar može da ima uvid u više nekretnina? I ako da, u čemu je onda suštinska razlika između vlasnika i stanara?

    Odgovor: Vlasnik vidi sve nekretnine, a stanar samo podskup nekretnina koje mu dodeli vlasnik ili admin. Stanaru može da se dodeli i da vidi sve nekretnine.

    Ostala ograničenja možete proizvoljno da stavite npr. vlasnik ne može da postane stanar, ali stanar koji je postao vlasnik može ponovo da se vrati samo na ulogu stanara; vlasnik može da pošalje zahtev za dodavanje novog objekta (nekretnine); vlasnik može da generiše izveštaj, a stanar ne itd.

47. **Pitanje:** Da li treba da omogućimo da jedan korisnik sistema može da bude npr. stanar u jednoj kući, da bude stanar u nekoj drugoj kući, da bude vlasnik u nekoj trećoj itd?

    Odgovor: Možete tako da implementirate, ali nije obavezno.

48. **Pitanje:** Da li je HTTPS obavezan za KT2?

    Odgovor: Ne, HTTPS bodujem na finalnoj odbrani.

49. **Pitanje:** Da li JWT token treba da se čuva u localStorage-u ili u sessionStorage-u?

    Odgovor: JWT čuvajte u session storage-u. Da biste videli razliku između local storage i session storage, ubacite proizvoljan string i u local i u session storage, zatvorite browser i pogledajte ponovo oba storage-a.

50. **Pitanje:** Da li vlasnik kuće može da dodaje stanara ili samo administrator?

    Odgovor: Obe opcije su prihvatljive.

51. **Pitanje:** Da li da imamo 3 uloge owner, tenent i nešto između owner-a i tenant-a, pa da taj između može ponovo da se vrati u tenant-a, ili da imamo samo 2 uloge?

    Odgovor: Možete da napravite 3 uloge u sistemu (npr. main owner, owner, tenant) i da razlika između owner-a i main owner-a bude to što main owner ne može da postane tenant i npr. on može da menja neke osnovne podatke, da pošalje adminu zahtev za dodavanje nekog novog uređaja ili slično, a običan owner ne može.

    Minimum je potrebno da imate admina, vlasnika i stanara, a sve ostale uloge u sistemu možete proizvoljno da izmodelujete.

52. **Pitanje:** Zanima me da li se pri blokiranju korisnika, on blokira da odredjeno vreme (npr 15min) ili je blokiran dok ga admin ne odblokira?

    Odgovor: Dovoljno je da ga blokirate na određeno vreme. Možete i da kombinujete te dve opcije koje ste naveli, npr. blokiramo korisnika na 15min i ako opet pravi greške onda mora adminu da se javi, da bi admin odblokirao nalog.

53. **Pitanje:** Da li kod druge tacke kod autentifikacije tj polisa za lozinku, da li se proverava format i pri registraciji i pri logovanju ili samo pri registraciji?

    Odgovor: Format proveravate prilikom registracije/dodavanja korisnika. Ako ste lozinku proverili prilikom dodavanja, kada se korisnik prijavljuje na sistem koristiće istu tu lozinku koja je već proverena.

54. **Pitanje:** Koji bi bili uslovi da se projekat iz bezbednosti odbrani ranije u ovom roku, ali samo za ocenu 6?

    Odgovor: Da biste položili praktičan deo ispita (projekat) dovoljno je da implementirate funkcionalnosti KT1 i da podignete HTTPS.

55. **Pitanje:** Da li proces registracije/dodavanja korisnika treba da povezujemo sa PKI delom aplikacije?

    Odgovor: Ne morate da povezujete ovaj deo sa PKI. PKI možemo da posmatramo kao odvojenu celinu. Ako želite, možete da uvežete sve u jedan proces.

56. **Pitanje:** Da li je potrebno implementirati promenu šifre korisnika?

    Odgovor: Ne, promena lozinke nije obavezna funkcionalnost.

57. **Pitanje:** Da li je potrebno implementirati izmenu podataka o korisniku?

    Odgovor: Ako mislite na osnovne podatke o korisniku, to nije obavezna funkcionalnost. Ima smisla da možemo da menjamo osnovne podatke o korisniku, pa ako želite možete to da implementirate.

    Promena uloge je neka vrsta izmene korisnika, tako da u tom kontekstu da.

58. **Pitanje:** Da li je za projekat iz predmate BSEP potrebno implementirati sve funkcionalnosti za kt2 i na aplikaciji za klijente koja trenutno nema nikakve funkcionalnosti ili se to može ostaviti za sledeću kontrolnu tačku?

    Odgovor: Ako mislite na admin aplikaciju, odgovor je da. Ako mislite pod “aplikacija za klijente” na aplikaciju Moja kuća, ima smisla i da je ovaj deo implementiran na toj aplikaciji.

    Za KT2 za funkcionalnosti autentifikacija i autorizacija nije eksplicitno navedeno “autentifikacija za admin aplikaciju” ili “autorizacija za admin aplikaciju”. Podrazumeva se da je za ceo sistem. U slučaju da neko nije

podigao aplikaciju Moja kuća neću skidati bodove, ali morate da imate način da mi demonstrirate da implementirani RBAC radi tj. da ne bude samo prolaz kroz kod.

59. **Pitanje:** Da li je potrebno i na klijentskoj strani implementirati login za ovu kt?

    Odgovor: Ako pod “klijentska strana” mislite na frontend odgovor je da (neki timovi su pod tim terminom mislili na Moja kuća aplikaciju, pa da ne bude zabune). Sve funkcionalnosti za KT2 treba podržati i na frontentu i na bekendu tj. klijentskoj i serverskoj strani.

60. **Pitanje:** Na šta se misli pod “validacija podataka i na klijentskoj i na serverskoj strani”?

    Odgovor: Sva polja treba da budu validirana na odgovarajući način. Najbolji pristup je whitelist tj. da napravite odgovarajuće regularne izraze za polja na klijentskoj (front) i serverskoj strani (back).

61. **Pitanje:** Da li logovi treba da se čuvaju u noSQL bazi.

    Odgovor: Da, logovi treba da se čuvaju u noSQL bazi.

62. **Pitanje:** Da li nova pravila za alarme moramo da dodajemo preko Rule-based sistema?

    Odgovor: Dovoljno je da inicijalno napravite u sistemu nekoliko pravila koja će ići preko Rule-based sistema. Ostala pravila možete proizvoljno da kreirate u aplikaciji, a isto tako i dodavanje novih pravila.

63. **Pitanje:** Šta konfiguracioni fajl sadrži i šta nama ti uređaji šalju?

    Odgovor: Konfiguracioni fajl koristimo da definišemo odakle ćemo čitati poruke koje uređaji generišu, da definišemo filter i period čitanja tih poruka. Uređaji šalju poruke, npr:

    poruka1: Lampa je ugašena

    poruka2: Temperatura je ispod 20 stepeni

    Inicijalno je predviđeno da uređaji sve poruke čuvaju u nekom fajlu i da na određeni vremenski period, i u skladu sa filterom, Moja kuća preuzima i obrađuje te poruke.

    Putanja u konfiguracionom fajlu u tom slučaju je putanja do tog fajla sa porukama.

    Period čitanja definiše kada će Moja kuća da preuzme nove poruke koje su sačuvane u fajlu sa porukama.

    Filter u vidu regexa koristimo da bismo preuzeli samo poruke koje zadovoljavaju određeni kriterijum. Uređaji sve vreme generišu različite poruke, a Moja kuća preuzima samo poruke koje prođu taj filter. Sve ostale poruke

Moja kuća ne obrađuje, tj. ne prikazuje korisniku, ne ulaze u izveštaj, niti okidaju alarme.

Konfiguracioni fajl može da se ručno podesi na početku, pre pokretanja sistema.

Takođe, ovaj deo može i na drugačiji način da se implementira. Npr. poruke čuvamo u bazi i imamo mogućnost da kroz UI dodamo nove uređaje, da ih povezujemo sa objektima, da definišemo period čitanja itd. U ovom slučaju putanja neće biti zaista putanja, već identifikator uređaja, a period čitanja i filter u vidu regexa treba da zadrže svoju funkciju.

Napomena: Uređaji generišu poruke i njih prati Moja kuća, a sve aplikacije u sistemu generišu logove i njih prati admin aplikacija.

64. **Pitanje:** Što se tiče regexa nije nam jasno šta tačno znači filter u vidu regexa u uređaju, to nas malo buni?

    Odgovor: Pogledati pitanje 63.

65. **Pitanje:** Da li nova pravila moraju preko template-a?

    Odgovor: Ne, nije obavezno. Dovoljno je da napravite 2-3 pravila preko drools-a, a sva ostala možete proizvoljno da kreirate. Dodavanje novih pravila ne mora da se radi preko template-a.

66. **Pitanje:** шта би требало да садрже извјештаји за Моја кућа апликацију? Да ли је то неки проценат везан за број активираних аларма или неки прикази аларма по појединачним уређајима у одређено временском периоду или нешто треће?

    Odgovor: Izveštaje generišete za određeni vremenski period i jedan izveštaj treba da sadrži osnovne informacije (vremenski period za koji se traži izveštaj, koji objekti i uređaji su obuhvaćeni tj. izlistati sve korisnikove, i eventualno ko je zahtevao izveštaj) i prikaz koliko alarma se u tom vremenskom periodu desilo. Ne morate da računate procente, dovoljno je da prikažete zbirno koliko ih je bilo po uređaju ili objektu. Ako je sve bilo u redu, onda treba da se prikaže rečenica koja informiše korisnika o tome ili da se prikaže da je bilo 0 alarma.

67. **Pitanje:** Koji je najbolji način za komunikaciju između uređaja i aplikacije? Da li da radimo nešto jednostavno pomoću baze/file ili nešto komplikovanije pomoću Message Queue?

    Odgovor: Lepo bi bilo da se ubaci neki Message Queue, ali nije obavezno da se tako nešto implementira na projektu. U realnom svetu koristili bismo MQTT. Za ovaj projekat je dovoljno da implementirate neko jednostavnije rešenje baza/fajl.

68. **Pitanje:** Datum odbrane projekta

    Odgovor: Za slučaj da neko nije video obaveštenje na enastavi, odbrana projekta je pomerena zbog prijemnog ispita na fakultetu. Pomerila sam i rok za poslednji commit. Datumi su navedeni u sekciji *Odbrana projekta* (pre sekcije sa pitanjima i odgovorima).

69. **Pitanje:** Za logove imamo samo pravilo ako je error da se okine alarm, ne znam kakvo bi jos admin mogao dodati za logove

    Odgovor: Admin za logove može da doda mnogo različitih pravila. Napravite formu koja će podržati da se alarmi kreiraju tako što se postave uslovi za više različitih parametara. Primeri:

    Bilo koji tip loga, npr. admin želi da dobije notifikaciju ako se desi log čiji je tip warning;

    Ako poruka loga sadrži neki string;

    Ako se log desio određenog datuma i vremena itd.

70. **Pitanje:** Da li je potrebno da ubacimo sokete kada se desi alarm ili je dovoljno da se javi na mejl?

    Odgovor: Da, notifikacija treba odmah da se prikaže korisniku, a ne da se izmene vide tek nakon refresh-a stranice. Ne morate da šaljete obaveštenje na mejl.

71. **Pitanje:**

    Odgovor:

72. **Pitanje:**

    Odgovor: