UNIVERZITET U NOVOM SADU
FAKULTET TEHNIČKIH NAUKA
NOVI SAD

Grupa 20
Elena Kevac PR145/2015
Maja Đorđević PR37/2015
Tanja Radojčić PR50/2015
Jelena Bajić PR73/2015

Zadatak 7

Sigurnost i bezbednost u elektroenergetskim sistemima

- Primenjeno softversko inženjerstvo -

Novi Sad, novembar 2018.

Sadrzaj

1. OPIS REŠAVANOG PROBLEMA

Zadatak projekta je pravljenje sigurnosne komunikacije između klijenta i servera za upravljanje pristupom sistemu fajlova.

Potrebno je bilo implementirati **HostProtection** i **ProxyProtection** komponente za hostovanje WCF servisa i uspostavljanje komunikacionog kanala sa istim.

HostProtection komunicira preko TCP protokola I može da podrži *Windows(Kerberos/NTLM)* autentifikaciju na dva nivoa: transportnom I na nivou poruka.

Korisnik je povezan sa privilegijama posredstvom *Windows* grupa koje su mu dodeljene tako
što podržava RBAC model autorizacije.U RBAC modelu grupe I permisije koje poseduje su:

- *Reader(Read,Access)*
- *Modifier(Read,Edit,Access) i*
- *Administrator(Read,Edit,Access,Administrate).*

Korisniku je ponuđen interfejs *IFileService* koji omogućava rad sa fajl sistemom.

Interfejs *IFileService* nudi sledeće metode:

- CreateFolder – *Administrate* privilegija
- CreateFile – *Read* privilegija
- ModifyFolderName – *Edit* privilegija
- ModifyFile – *Edit* privilegija
- Read – *Read* privilegija
- DeleteFolder – *Administrate* privilegija
- DeleteFile – *Administrate* privilegija

Projekat takođe podržava zapis događaja u specifični *Windows Event Log* kao I zapis svake izmene konfiguracije od strane svih servisa u okviru *Syslog* komponente za centralizovano logovanje u **HostProtection** sistemu.

Za svaki poziv metode, umesto kreiranja *IPrincipal* objekta što je standardno, obezbeđeno je *in-memory* keširanje kao I osvežavanja u slučaju izmene RBAC konfiguracije.

2. TEORIJSKE OSNOVE

"**AAA**" (eng. AAAs of security) predstavlja akronim za tri osnovna bezbednosna mehanizma koji zajedno funkcionišu kako bi se obezbedio kontrolisan pristup informacionom sistemu i podacima (eng. AAA = *Authentication, Authorization, Accounting=Auditing*). *Auditing* se odnosi na proces praćenja, snimanja/logovanja, analize i izveštavanja o bezbednosnim događajima u sistemu.

Korišćeni bezbednosni mehanizam za autentifikaciju je *Windows*(*Kerberos/NTLM*) autentifikacija na dva nivoa: na transportnom nivou i na nivou poruka.

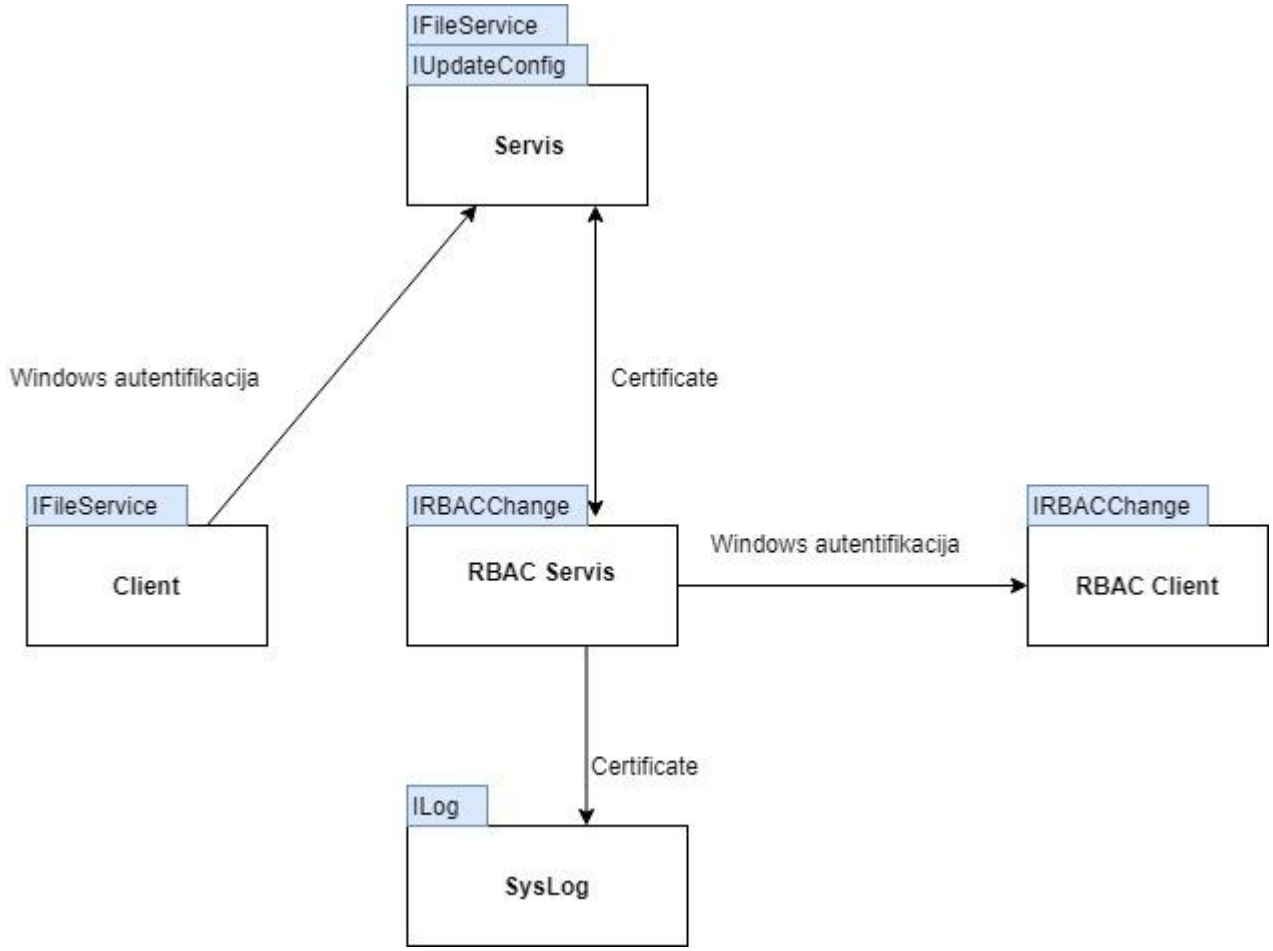
NTLM (NT Lan Manager) je autentifikacioni protokol zasnovan na *challenge-response* autentifikacionoj šemi, čime je omogućena autentifikacija bez slanja poverljivih podataka (šifre). Iako challenge-response spada u jake autentifikacione šeme jer nema razmene poverljivih podataka, problem ovakvih protokola je činjenica da servis mora da zna originalnu šifru svakog klijenta kako bi mogao da validira pristigli response. Dodatno, u ovako definisanom autentifikacionom protokolu izostaje verifikacija servisnog identiteta od strane klijenta, odnosno ovakav protokol ne omogućuje obostranu autentifikaciju

Kerberos je dvosmerni autentifikacioni protokol se zasniva na trećoj strani od poverenja i razmeni ticketa u cilju uspostavljanja bezbedne obostrane autentifikacije učesnika u komunikaciji bez razmene šifri. Kako bi se obezbedili sigurniji protokoli, uvodi se treća strana od poverenja odnosno entitet kome veruju svi ostali učesnici u komunikaciji.

Bezbednosni događaji mogu biti kako uspešno izvršene akcije u sistemu, tako i neuspešni pokušaji pristupa resursima. Audit log predstavlja zapis bezbednosno relevantnih događaja u sistemu. S obzirom da audit log predstavlja vremenski obeležene zapise o aktivnostima u sistemu, učesnici ne mogu naknadno poricati izvršene akcije čime se obezbeđuje neporecivost. Integritet, odnosno tačnost podataka koje sadrže audit logovi se obezbeđuje primenom mehanizama kontrole pristupa logovima, digitalnim potpisima, itd. Analizom prikupljenih informacija moguće je detektovati kako uspešne tako i neuspešne pokušaje kako redovnih tako i malicioznih aktivnosti u sistemu, odnosno naknadno utvrditi uzroke grešaka ili otkaza u sistemu.
Korišćeni bezbednosni mehanizam za logovanje je *Windows Event Log*. Ugrađeni .NET mehanizam za logovanje i audit koristi log datoteke *Windows* operativnog sistema za zapis različitih tipova događaja: sistemskih (generisanih od strane operativnog sistema), aplikativnih i bezbednosnih – tzv. *Microsoft Windows Event Log*.

Korišćeni bezbednosni mehanizam za autorizaciju je **RBAC** autorizaciona šema. Kontrola pristupa zasnovana na ulozi (**RBAC**) je neutralan mehanizam kontrole pristupa koji je definisan ulogama i privilegijama. Komponente RBAC-a, kao što su dozvole i uloge korisnika, olakšavaju izvršavanje korisničkih zadataka. Upotrebom RBAC-a olakšava se upravljanje korisničkim privilegijama.

3. DIZAJN IMPLEMENTIRANOG SISTEMA



Slika 1. Dizajn sistema

Komponente sistema su:

- Servis
- Client
- RBAC Servis
- RBAC Client
- SysLog
- Biblioteke

Komunikacija svih komponenti se vrši preko WCF komunikacije.

Servis implementira *IFileService* interfejs koji izlaže metode **Clientu** i to metode za rad sa fajlovima. Pored toga implementira i *IUpdateConfig* koji služi kao metoda koju poziva **RBAC Servis** u slučaju izmene konfiguracije, kako bi obavestio servera da se izmena desila I da je potrebno *update*-ovati permisije klijenata.

Komunikacija **Servisa** I **Clienta** odvija preko TCP protokola i *Windows* autentifikacije odnosno preko NTLM protokola, dok njegova komunikacija sa **RBAC Servisom** se odvija posredstvom sertifikata.

Client bira nivo na kom će komunicirati sa servisom i koristi metode izložene preko *IFileService* interfejsa.

RBAC Servis izlaže *IRBACChange* interfejs za **RBAC Client**-a koji upisuje promene koje je **RBAC Client** uneo. Ponaša se i kao klijent za **Servis** i poziva metodu *UpdateConfig* koja mu je izložena nakon promene od **RBAC Clienta** kako bi obavestio **Servis**, kao i za **SysLog** gde poziva metode za logovanje događaja.

Komunikaciju sa **RBAC Clientom** uspostavlja preko *Windows* autentifikacije kao i **Client** i **Servis**, dok komunikaciju sa **Servisom** I **SysLogom** uspostavlja preko sertifikata.

RBAC Client koristi metodu izloženu preko *IRBACChange* I menja konfiguraciju resx fajla u kom se nalazi konfiguracija grupa i permisija.

SysLog izlaže ILog interfejs za RBAC Servis koji loguje promene.

4. TESTIRANJE SISTEMA

- **Pozitivni test scenariji**

1. Izbor na kom nivou radi server i klijent

Ako pri izboru nivoa na serveru I klijentu se izabere isti nivo, njihova komunikacija se uspešno uspostavlja i klijentu se izlaže meni za izbor akcija.

2. Permisije klijenta

Ako klijent izborom iz menija izabere funkciju za koju ima određenu dozvolu, funkcija će biti izvršena.

3. Promena konfiguracije

Ako RBAC klijent uspešno promeni konfiguraciju, RBAC server javlja serveru i pokreće UpdateConfig metodu koja updatuje sve permisije klijenata koji su pokrenuti kako bi klijent nastavio rad sa novom konfiguracijom i upisuje to u event log.

- **Negativni test scenariji**

1. Izbor na kom nivou radi server i klijent

Ako pri izboru nivoa na serveru se izabere jedan, a na klijentu drugi nivo desi se `CommunicationException` koji se obrađuje na klijentu.

2. Permisije klijenta

Ako klijent izborom iz menija izabere funkciju za koju nema određenu dozvolu,desi se `SecurityException` koji se obrađuje na serveru.

3. Promena konfiguracije

Ako RBAC klijent pokuša da promeni konfiguraciju ali dođe do greške, desi se `CommunicationException` koji se obrađuje na RBAC klijentu.