ELEKTROENERGETSKI SOFTVERSKI INŽENJERING, FTN NOVI SAD

Dokumentacija projektnog zadatka br. 8

Sigurnost i bezbednost elektroenergetskog softvera

Srđan Punović E3 8/2016 *Marko Bogdanović E3 4/2016*

Novembar 2016

Opis problema

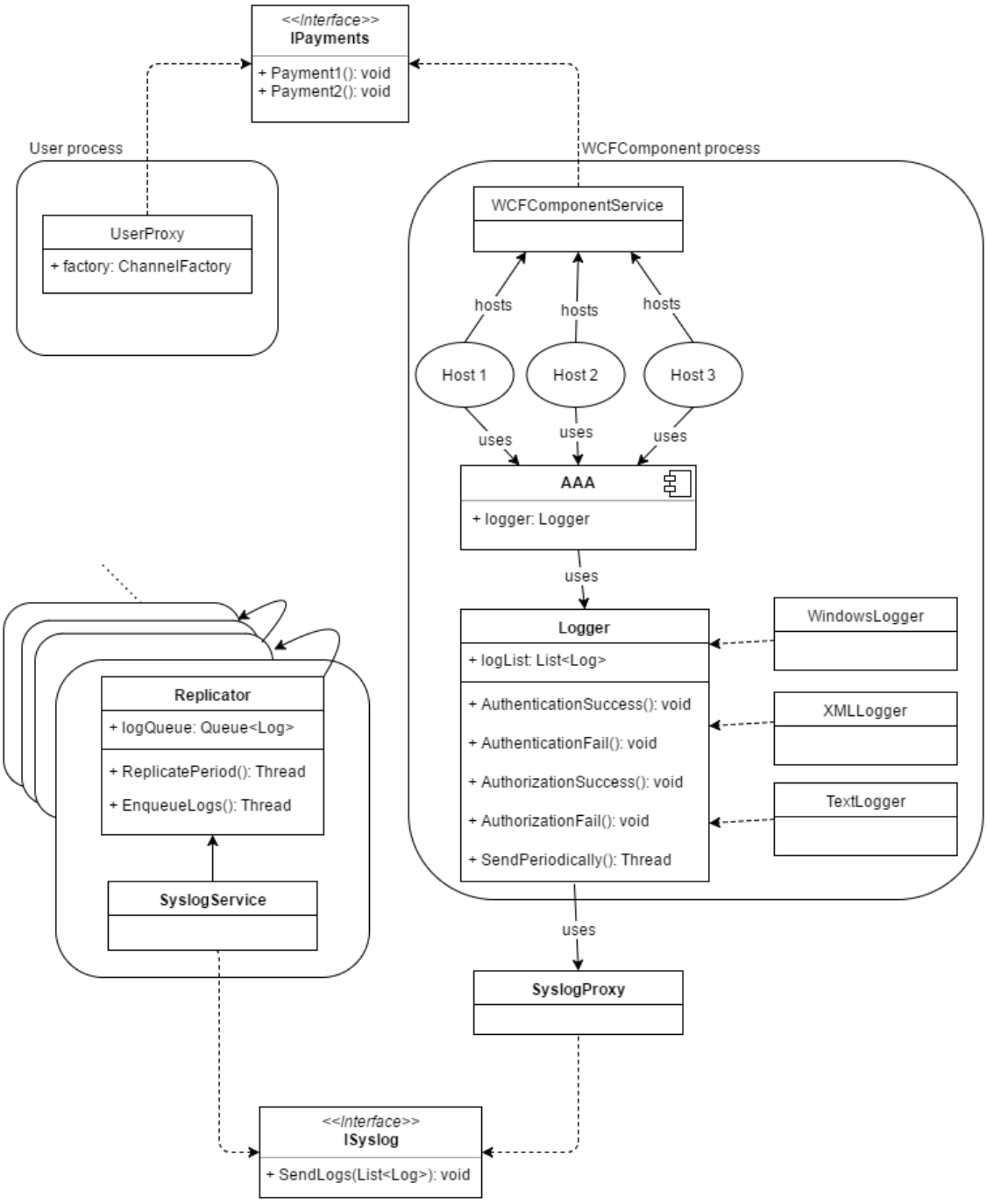
Implementirati servis koji ima ulogu Syslog servera. Syslog server je komponenta koja u standardnom syslog formatu zapisuje događaje pristigle od različitih Syslog klijenata sa kojima komunicira preko TCP protokola (default port je 514). Autentitikacija izmedu Syslog servera i klijenta vrši se pomoću sertifikata. Ulogu Syslog klijenta imaju tri komponente koje svojim klijentima pružaju usluge definisane interfejsom IPayments koji pruža usluge uplate i isplate na korisničke račune. Ove tri komponente se razlikuju samo u načinu zapisivanja relevantnih događaja u sistemu:

- WCFComponent_1 loguje u tekstualni fajl
- WCFComponent_2 loguje u Windows Event Log
- WCFComponent_3 loguje u XML fajl

Relevantni bezbednosni dogadaji su (uspešni i neuspešni) pokušaji poziva metoda IPayments interfejsa. Da bi klijent mogao da vrši uplate i isplate, mora da bude član Windows grupe "AccountUsers". Komunikacija izmedu ove komponente i njegovih klijenata vrgi se preko TCP protokola (pomoću sertitikata).

Poruke upisane u interni log fajl se ne prosleđuju pojedinačno Syslog serveru, već svaka komponenta buffer-uje događaje i isporučuje ih Syslog serveru periodično npr. period od 1 min). Syslog server komponenta loguje bezbednosne dogadaje WCFComponent_1, WCFComponent_2 i WCFComponent_3 u jedinstvenoj bazi podataka prema Timestampu. Dodatno, Syslog server treba da omogući repliciranje podataka na backup Syslog server. Backup syslog poruka se vrši periodično. Potrebno je obezbediti obostranu Windows autentiitkaciju sa backup Syslog komponentom.

Dizajn programskog rešenja



Dijagram 1. Dizajn programskog rešenja

U ovom radu uvedene su tri vrste procesa: User, WCFComponent i Syslog. User komponenta ima ulogu klijenta na WCFComponent servis koji implementira IPayments interfejs. U okviru WCFComponent procesa istoimeni servis je pokrenut u okviru tri hosta. Svaki od njih koristi AAA modul za bezbednosne mehanizme. AAA modul sadrži Logger koji može biti TextLogger, XMLLogger ili WindowsLogger. Za svaki host zadužen je različit tip logera. Svaki loger preko interfejsa ISyslog, periodično šalje sve logove, koje je prethodno interno skladištio, Syslog servisu koji je pokrenut u okviru jednog od Syslog procesa. Jedan Syslog servis je zadužen za prethodnu komunikaciju dok su ostali zaduženi za replikaciju podataka. Komunikacija User -> WCFComponent i WCFComponent -> Syslog obezbeđena je uz pomoć sertifikata. Korisnik koji je pokrenuo User proces mora biti pripadnik AccountUsers grupe.

Rezultati testiranja

Prethodno pomenuto programsko rešenje testirano je sledećim scenarijima:

- Nevalidni User sertifikat
- Validni User sertifikat bez grupe AccountUsers
- Validni User sertifikat sa grupom AccountUsers

U prvom slučaju pristup je onemugućen jer sertifikati sa obe strane nisu izdati od istog CA.
U drugom slučaju takođe jer korisnik nije član grupe AccountUsers
U trećem slučaju korisnik se uspešno autentifikovao i autorizovao.

Svi prethodno navedeni bezbednosni događaji prosleđeni su Syslog serveru u odgovarajućem formatu.

Zaključak

U ovom radu izloženi su neki od bezbednosnih mehanizama modernih distribuiranih aplikacija. U okviru WCF .NET okruženja, korišćeni su mehanizmi autentifikacije, autorizacije i auditinga. Kao platformski nezavistan oblik razrešavanja prethodno pomenutih bezbednosnih pitanja korišćeni su sertifikati.