



UNIVERZITET U NOVOM SADU
FAKULTET TEHNIČKIH NAUKA
NOVI SAD



Grupa 5

Jovan Davidović, PR 13/2015

Slobodan Brdar, PR 14/2015

Dunja Bursać, PR 22/2015

Dimitrije Mitić, PR 27/2015

Zadatak 18

Sigurnost i bezbednost u elektroenergetskim
sistemima

- Primenjeno softversko inženjerstvo -

Novi Sad, 13. novembar 2018.

Sadržaj

1. OPIS REŠAVANOG PROBLEMA	3
2. TEORIJSKE OSNOVE	4
3. DIZAJN IMPLEMENTIRANOG SISTEMA	6
4. TESTIRANJE SISTEMA	9

1. OPIS REŠAVANOG PROBLEMA

Implementacija servisa koji ima ulogu Malware Scanning alata (**MST**). MST komponenta po svom pokretanju kreira posebnu nit koja periodično (svakih N sekundi koje se podešavaju u konfiguraciji) prolazi kroz listu trenutno aktivnih procesa i proverava imali nedozvoljenih. Nedozvoljeni procesi se definišu u unapred popunjenoj listi (Backlist.xml konfiguraciji) kao proces pokrenut pod određenim korisničkim nalogom ili nalogom koji pripada određenoj korisničkoj grupi.

MST komunicira sa sistemom za prevenciju napada – Intrusion Prevention System (**IPS**) preko sertifikata. MST komponenta ima zadatak da po detekciji neovlašćeno pokrenutog procesa pošalje alarm IPS komponenti. IPS komponenta evidentira nivo kritičnosti prijavljenih procesa i vreme detekcije. Nivoi kritičnosti su: INFORMATION, WARNING i CRITICAL. Kada proces dostigne nivo kritičnosti CRITICAL, IPS komponenta šalje zahtev za gašenje tog procesa MST komponenti. MST i IPS komponente komuniciraju preko sertifikata. Svaka promena nivoa kritičnosti se beleži u Windows Event Log-u.

Obezbeđuje se provera integriteta blacklist konfiguracije tako da se svaka ručna izmena fajla smatra za nevalidnu, a samo autorizovanim pozivom metode MST servisa je moguće napraviti validnu izmenu.

2. TEORIJSKE OSNOVE

Za izradu projekta korišćeni su sledeći bezbedonosni mehanizmi:

- WCF komunikacija preko sertifikata
- Provera integriteta blacklist konfiguracionog fajla
- Opšta konfigurabilnost (adrese, nazivi sertifikata i sl.)

WCF komunikacija preko sertifikata

Kako bi se obezbedila adekvatna autentifikacija učesnika u komunikaciji između MST i IPS komponenti korišćeni su sertifikati: RootCert, MSTCert i IPSCert.

- **RootCert** – sastoji se od privatnog i javnog dela sertifikata (RootCert.pvk i RootCert.cer) i predstavlja samopotpisani sertifikat čiji se javni deo instalira u *Trusted Root Certification Authorities (TRCA)* folderu na svim računima gde je potrebno obezbediti komunikaciju preko sertifikata. Ostali sertifikati se potpisuju njegovim privatnim ključem, dok komponente koje komuniciraju proveravaju verodostojnost sertifikata preko kojih se ostvaruje komunikacija pomoću javnog dela RootCert-a koji imaju instaliran u *TRCA* folderu (primenjujući ChainTrust princip).
- **MSTCert** – sastoji se od privatnog i javnog dela sertifikata MST sertifikata (MSTCert.pvk i MSTCert.cer fajlova). Mašina na kojoj se pokreće MST komponenta imaće instaliran MSTCert.pfx fajl (koji predstavlja privatni i javni deo sertifikata) u svom *Personal* folderu. Mašina na kojoj se pokreće IPS komponenta imaće instaliran MSTCert.cer (samo javni deo sertifikata) u svom *Trusted People* folderu.
- **IPSCert** - sastoji se od privatnog i javnog dela sertifikata IPS sertifikata (IPSCert.pvk i IPSCert.cer fajlova). Mašina na kojoj se pokreće IPS komponenta imaće instaliran IPSCert.pfx fajl (koji predstavlja privatni i javni deo sertifikata) u svom *Personal* folderu. Mašina na kojoj se pokreće MST komponenta imaće instaliran IPSCert.cer (samo javni deo sertifikata) u svom *Trusted People* folderu.

U primeru komunikacije u kojoj MST komponenta predstavlja klijenta, a IPS komponenta server upotreba sertifikata je sledeća: MST-u je od značaja IPS-ov javni deo sertifikata, a IPS-u njegov privatni deo sadržan u .pfx fajlu.

U primeru komunikacije u kojoj IPS komponenta predstavlja klijenta, a MST komponenta server upotreba sertifikata je sledeća: IPS-u je od značaja MST-ov javni deo sertifikata, a MST-u njegov privatni deo sadržan u .pfx fajlu.

Provera integriteta blacklist konfiguracionog fajla

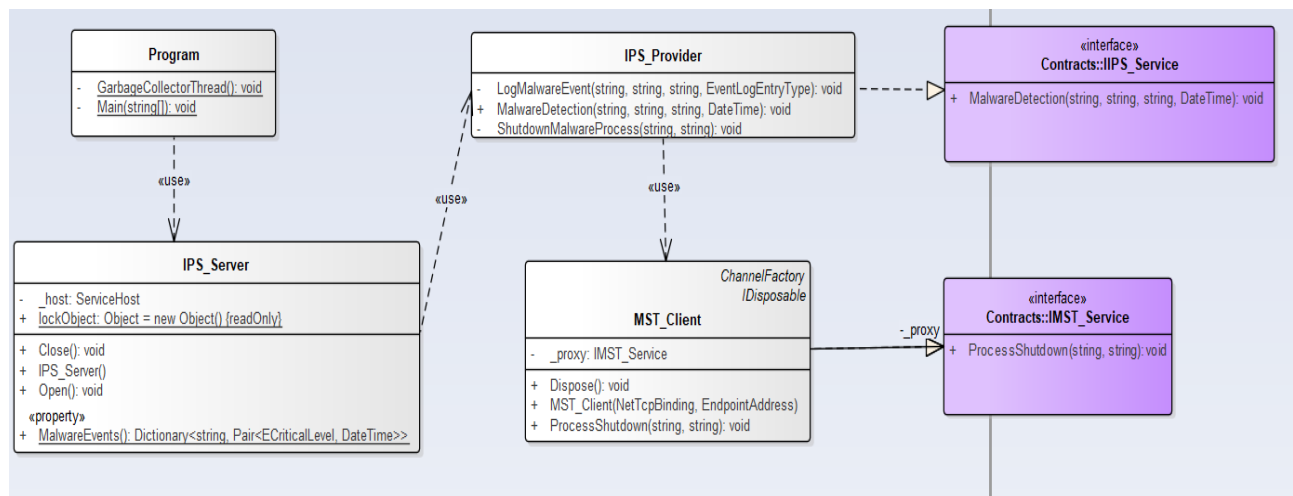
Upotrebom ugrađene .NET funkcije GetHashCode() izračunava se heš vrednost konfiguracionog fajla koja se potom upisuje u lokalnu promenljivu MST komponente. Prilikom čitanja iz blacklist.xml fajla ili na zahtev, heš vrednost se izračunava na isti način i poredi sa vrednošću sačuvanoj u lokalnoj promenljivoj. Ukoliko se ručno (neovlašćeno) izmeni konfiguracioni fajl, prilikom narednog pristupa fajlu provera će pokazati da je .xml fajl korumpiran.

Opšta konfigurabilnost

Svi osetljivi parametri (adrese, nazivi sertifikata i sl.) se ne nalaze zakodirani u .cs fajlovima već su izdvojeni u App.config fajlove odakle se ištitavaju. Pored toga što se olakšava izmena ovih paramatera, obezbeđuje se i njihova zaštita od maliciozne upotrebe. Sadržaj ovih fajlova je moguće i dodatno zaštititi.

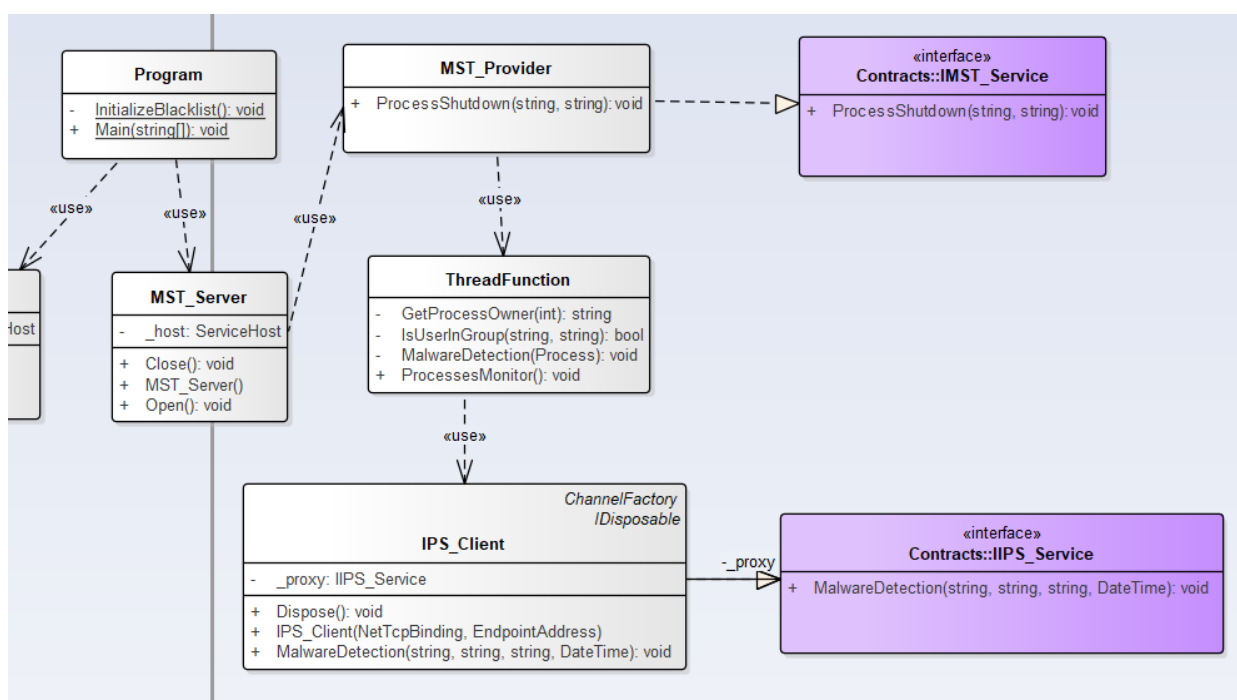
3. DIZAJN IMPLEMENTIRANOG SISTEMA

Komunikacija MST (klijent), IPS (server)



Kao što se može videti na priloženoj slici `IPS_Server` izlaže implementiranu metodu `IIPS_Service`-a. U okviru te metode se evidentira maliciozni proces na osnovu prosleđenih parametara (`userID`, `processed`, `processName`, `timeOfDetection`). Kao što je opisano u odeljku 1, po prelasku određenog procesa u `CRITICAL` stanje formira se zahtev za njegovo gašenje, koji je enkapsuliran metodom `ProcessShutdown` `MST_Client` klase čije je zaduženje da inicijalizuje WCF komunikacioni kanal ka `MST` komponenti.

Komunikacija IPS(klijent), MST(mst server)



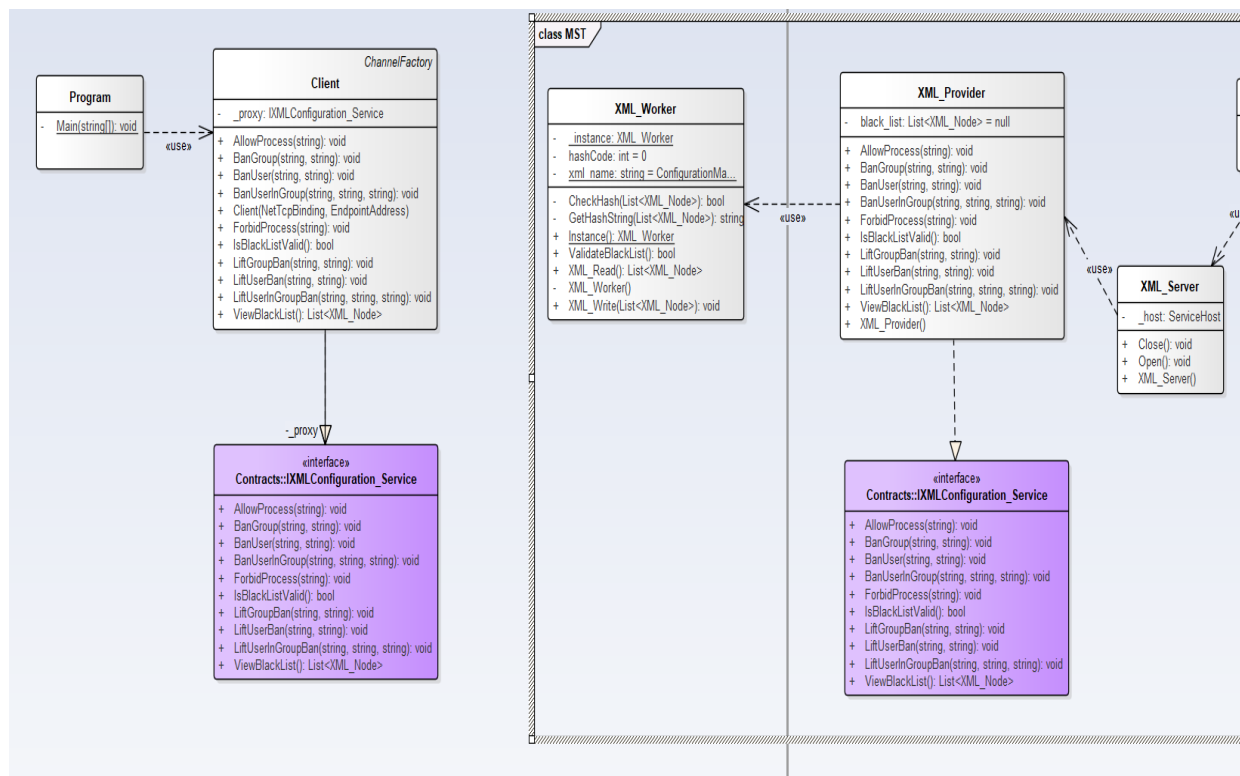
Kao što se može videti na priloženoj slici **MST_Server** izlaže implementiranu metodu **IMST_Service**-a. U okviru te metode se proces sa naznačenim **processID**-jem gasi. Kao što je opisano u odeljku 1, po detekciji malicioznog procesa (informacije o aktivnim procesima se periodično upoređuju sa opisom malicioznih procesa iz blacklist-e) formira se zahtev za njegovim evidentiranjem koji je enkapsuliran metodom **MalwareDetection** **IPS_Client** klase čije je zaduženje da inicijalizuje WCF komunikacioni kanal ka IPS komponenti.

IPS i MST komponente komuniciraju preko WCF kanala uz korišćenje sertifikata, kao što je objašnjeno u odeljku 2.

Komunikacija Client(xml klijent), MST(xml server)

Na MST komponenti se podiže host koji izlaže metode iz IXMLConfiguration_Service interfejsa.

To su metode koje obezbeđuju validne izmene blacklist xml fajla. Client komponenta obezbeđuje jednostavan console meni za izbor izmena na xml fajlu. Ova komunikacija ka MST skomponenti se ne realizuje preko sertifikata.



(Uz projekat je prilože SBES1819_MST.EAP fajl iz kojeg su i uzimani screenshot-ovi.)

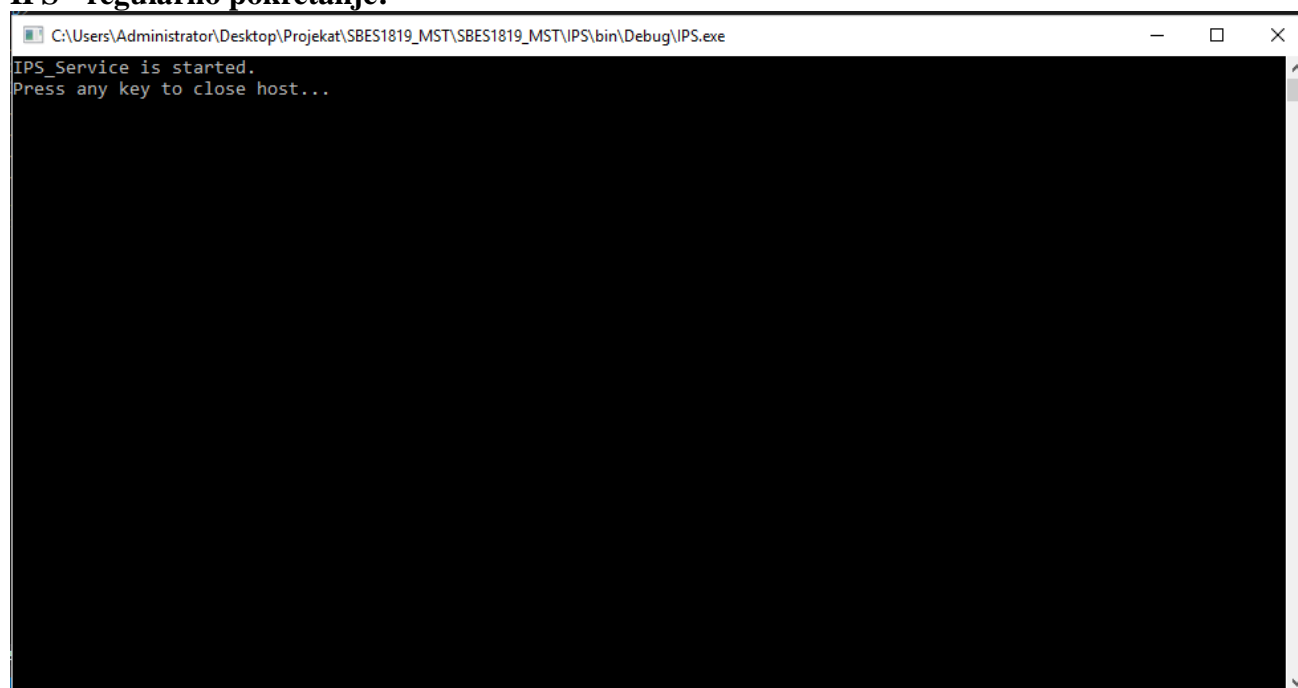
4. TESTIRANJE SISTEMA

Kao dokaz validnosti rešenja biće korišćeni sledeći slučajevi:

1. Pokretanje procesa od strane korisnika koji se nalazi na black list-i
2. Pokretanje procesa od strane korisnika koji je u grupi koja se nalazi na black list-i
3. Pokretanje procesa od strane određenog korisnika iz određene grupe, gde se ova kombinacija nalazi u black list-i
4. Ručna izmena black liste i provera validnosti na zahtev

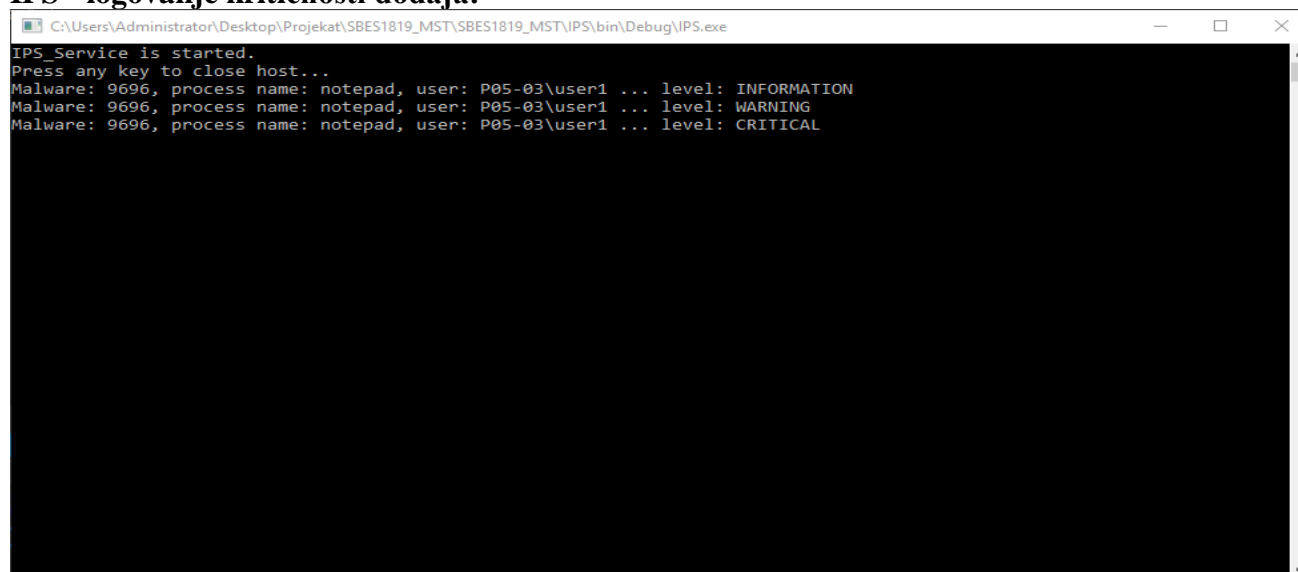
Ne gubeći na opštosti, prilikom testiranja koristiće se program koji pokreću jedan proces, jer neki složeni programi poput Google Chroma pokreću više procesa koji se kasnije moraju zatvarati u određenom redosledu, koji varira od programa do programa, te nam nije poznat.

IPS - regularno pokretanje:



```
C:\Users\Administrator\Desktop\Projekat\SBES1819_MST\SBES1819_MST\IPS\bin\Debug\IPS.exe
IPS_Service is started.
Press any key to close host...
```

IPS - logovanje kritičnosti dodaja:



```
C:\Users\Administrator\Desktop\Projekat\SBES1819_MST\SBES1819_MST\IPS\bin\Debug\IPS.exe
IPS_Service is started.
Press any key to close host...
Malware: 9696, process name: notepad, user: P05-03\user1 ... level: INFORMATION
Malware: 9696, process name: notepad, user: P05-03\user1 ... level: WARNING
Malware: 9696, process name: notepad, user: P05-03\user1 ... level: CRITICAL
```

IPS – greška prilikom neuspješne autentifikacije (nepostojanje adekvatnog root-a)

```
C:\Users\Administrator\Desktop\Projekat\SBES1819_MST\SBES1819_MST\IPS\bin\Debug\IPS.exe
Error on 'host.Open()'. Error message: The service certificate is not provided. Specify a service certificate in Service
Credentials.
[STACK_TRACE] at System.ServiceModel.Security.ServiceCredentialsSecurityTokenManager.CreateServerX509TokenProvider()
at System.ServiceModel.Security.ServiceCredentialsSecurityTokenManager.CreateLocalSecurityTokenProvider(RecipientServ
iceModelSecurityTokenRequirement recipientRequirement)
at System.ServiceModel.Security.ServiceCredentialsSecurityTokenManager.CreateSecurityTokenProvider(SecurityTokenRequi
rement requirement)
at System.ServiceModel.Channels.SslStreamSecurityUpgradeProvider.CreateServerProvider(SslStreamSecurityBindingElement
bindingElement, BindingContext context)
at System.ServiceModel.Channels.SslStreamSecurityBindingElement.BuildServerStreamUpgradeProvider(BindingContext conte
xt)
at System.ServiceModel.Channels.ConnectionOrientedTransportChannelListener..ctor(ConnectionOrientedTransportBindingEl
ement bindingElement, BindingContext context)
at System.ServiceModel.Channels.TcpChannelListener..ctor(TcpTransportBindingElement bindingElement, BindingContext co
ncontext)
at System.ServiceModel.Channels.TcpTransportBindingElement.BuildChannelListener[TChannel](BindingContext context)
at System.ServiceModel.Channels.BindingContext.BuildInnerChannelListener[TChannel]()
at System.ServiceModel.Channels.SslStreamSecurityBindingElement.BuildChannelListener[TChannel](BindingContext context
)
at System.ServiceModel.Channels.BindingContext.BuildInnerChannelListener[TChannel]()
at System.ServiceModel.Channels.MessageEncodingBindingElement.InternalBuildChannelListener[TChannel](BindingContext c
oncontext)
at System.ServiceModel.Channels.BinaryMessageEncodingBindingElement.BuildChannelListener[TChannel](BindingContext con
text)
at System.ServiceModel.Channels.BindingContext.BuildInnerChannelListener[TChannel]()
at System.ServiceModel.Channels.TransactionFlowBindingElement.BuildChannelListener[TChannel](BindingContext context)
at System.ServiceModel.Channels.BindingContext.BuildInnerChannelListener[TChannel]()
at System.ServiceModel.Channels.Binding.BuildChannelListener[TChannel](Uri listenUriBaseAddress, String listenUriRela
tiveAddress, ListenUriMode listenUriMode, BindingParameterCollection parameters)
at System.ServiceModel.Description.DispatcherBuilder.MaybeCreateListener(Boolean actuallyCreate, Type[] supportedChan
```

MST – regularno pokretanje

```
C:\Users\Administrator\Desktop\Projekat\SBES1819_MST\SBES1819_MST\MST\bin\Debug\MST.exe
MST_Service is started.
XML_Service is started.
Press any key to close all hosts...
Process: WUDFHost, process user: NO OWNER
Process: chrome, process user: NO OWNER
Process: conhost, process user: P05-03\Administrator
Process: mmc, process user: P05-03\Administrator
Process: svchost, process user: NO OWNER
Process: chrome, process user: NO OWNER
Process: WINWORD, process user: P05-03\Administrator
Process: conhost, process user: P05-03\Administrator
Process: MySQLNotifier, process user: P05-03\Administrator
Process: dwm, process user: NO OWNER
Process: SecurityHealthService, process user: NO OWNER
Process: svchost, process user: NO OWNER
Process: svchost, process user: NO OWNER
Process: svchost, process user: NO OWNER
Process: chrome, process user: NO OWNER
Process: chrome, process user: NO OWNER
Process: MST, process user: P05-03\MSTServer
Process: svchost, process user: NO OWNER
Process: conhost, process user: P05-03\MSTServer
Process: svchost, process user: NO OWNER
Process: Memory Compression, process user: NO OWNER
Process: chrome, process user: P05-03\Administrator
Process: chrome, process user: NO OWNER
Process: svchost, process user: NO OWNER
Process: svchost, process user: NO OWNER
Process: jusched, process user: P05-03\Administrator
```

MST – listanje aktivnih procesa

```
C:\Users\Administrator\Desktop\Projekat\SBES1819_MST\SBES1819_MST\MST\bin\Debug\MST.exe
Process: svchost, process user: NO OWNER
Process: dllhost, process user: NO OWNER
Process: svchost, process user: NO OWNER
Process: sihost, process user: P05-03\Administrator
Process: svchost, process user: NO OWNER
Process: svchost, process user: NO OWNER
Process: svchost, process user: NO OWNER
Process: svchost, process user: NO OWNER
Process: svchost, process user: NO OWNER
Process: taskhostw, process user: P05-03\Administrator
Process: svchost, process user: NO OWNER
Process: ServiceHub.VSDetouredHost, process user: P05-03\Administrator
Process: csrss, process user: NO OWNER
Process: igfxEM, process user: P05-03\Administrator
Process: svchost, process user: NO OWNER
Process: chrome, process user: NO OWNER
Process: chrome, process user: NO OWNER
Process: svchost, process user: NO OWNER
Process: svchost, process user: NO OWNER
Process: mmc, process user: P05-03\Administrator
Process: fontdrvhost, process user: NO OWNER
Process: svchost, process user: NO OWNER
Process: svchost, process user: NO OWNER
Process: svchost, process user: NO OWNER
Process: System, process user: NO OWNER
Process: Idle, process user: NO OWNER

***** END OF PASS *****
```