

Osnove informacione bezbednosti u infrastrukturnim sistemima

Projektni zadatak 22

Članovi tima:

Luka Đelić PR60/2020

Stefan Malinović PR62/2020

Stefan Milovanović PR68/2020

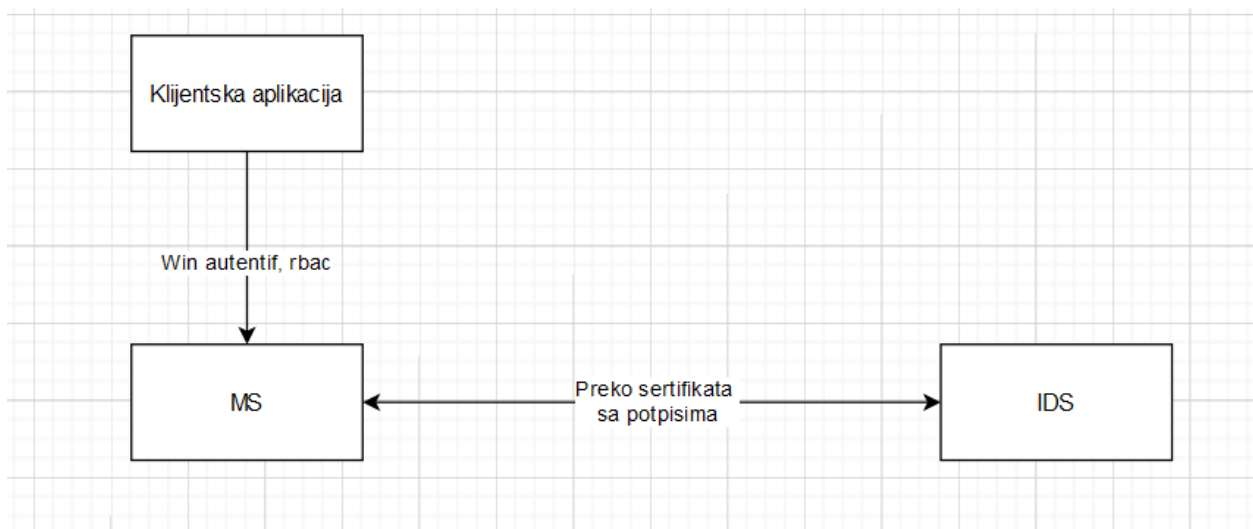
Srđan Mladenović PR72/2020

Asistent:

Zorana Babić

Opis sistema

Malware Scanning alat je sistem koji služi za proveravanje dozvoljenih procesa među trenutno aktivnim. Aktivira se periodično i proverava procese na osnovu konfiguracije sa nedozvoljenim procesima. Ukoliko naiđe na takav proces šalje alarm Intrusion Detection System komponenti koja loguje kritične događaje. Postoji i posebna komponenta klijent koja služi za izmenu konfiguracije.



Opis komponenti

Malware scanning

Malware Scanning (MS) servis je glavna komponenta sistema. Komunicira sa klijentskom aplikacijom kao server i sa IDS komponentom kao klijent. Služi za praćenje procesa aktiviranjem na svakih N sekundi. Ukoliko naiđe na nedozvoljeni proces automatski šalje alarm IDS-u. Da bi se za početak započela komunikacija između ove dve komponente potrebno je da imaju instalirane sertifikate, konkretno "wcfclient" i "wcfservice" sertifikate.

```
C:\Users\Administrator\Documents\OIBIS-Test\OIBISProjekat\MalwareScanner\bin\Deb...
Servis je uspesno pokrenut na adresi net.tcp://localhost:4000/IChangeConfig
DESKTOP-AV2PARO\WCFCClient
DESKTOP-AV2PARO\WCFCClient
-----
Choose option:
1) Request integrity breach report
Your Option --->
```

MS je zadužen da i sam loguje kritične događaje u svojoj log datoteci u Windows Event Log.

MalwareScannerApp Number of events: 488

Level	Date and Time	Source	Event ID	Task Category
Warning	1/15/2024 5:41:02 PM	Manager.AuditMS	0	None
Information	1/15/2024 5:40:29 PM	Manager.AuditMS	0	None
Information	1/15/2024 5:40:27 PM	Manager.AuditMS	0	None
Information	1/15/2024 5:39:51 PM	Manager.AuditMS	0	None
Information	1/15/2024 5:39:50 PM	Manager.AuditMS	0	None
Information	1/15/2024 5:39:46 PM	Manager.AuditMS	0	None
Information	1/15/2024 5:38:20 PM	Manager.AuditMS	0	None

Event 0, Manager.AuditMS

General Details

User Engineer1 successfully accessed to <http://tempuri.org/IChangeConfig/ReadConfiguration>.

Log Name: MalwareScannerApp

Source: Manager.AuditMS

Event ID: 0

Level: Information

User: N/A

OpCode: Info

More Information: [Event Log Online Help](#)

Logged: 1/15/2024 5:40:29 PM

Task Category: None

Keywords: Classic

Computer: DESKTOP-AV2PARO

Dodatno, da bi IDS prihvatio poruku potrebno je da on sadrži i digitalni potpis kojim se obezbeđuje integritet i autentičnost poruke, kao i neporecivost od strane pošiljaoca da je upravo on poslao poruku. Naime, digitalni potpis predstavlja hash vrednost izračunatu nad sadržajem poruke koja se zatim kriptuje privatnim ključem pošiljaoca. Primalac poruke, dekriptovanjem digitalnog potpisa javnim ključem pošiljaoca potvrđuje autentičnost poruke, jer samo pošiljalac ima odgovarajući privatni ključ. Ovim je istovremeno omogućeno da pošiljalac neće moći da porekne da je on poslao poruku.

Sa MS-a se može tražiti i provera integriteta log fajla koju proverava IDS:

```
Choose option:
1) Request integrity breach report
Your Option ---> 1
15. 1. 2024. 17:33:51 | Integrity Breached
15. 1. 2024. 17:33:57 | Integrity Breached
-----
```

Intrusion Detection System

Intrusion Detection System (IDS) je komponenta sistema koja loguje alarme koje dobija od MS-a na ranije objašnjen način. Log sadrži datum i vreme detekcije, naziv procesa i jedan od 3 nivoa kritičnosti - Information (proces detektovan prvi put), Warning (proces detektovan drugi put) ili Critical (proces detektovan više puta).

```
24. 12. 2023. 21:03:23 | svchost | Critical
15. 1. 2024. 17:27:43 | git-bash | Information
15. 1. 2024. 17:27:43 | bash | Information
15. 1. 2024. 17:27:43 | bash | Warning
15. 1. 2024. 17:27:46 | git-bash | Warning
15. 1. 2024. 17:27:46 | bash | Critical
```

Klijent

Klijentska aplikacija ima ulogu samo u izmeni blacklist malware konfiguracije. Klijenta pokreću korisnici koji, da bi uopšte mogli da pristupe MS-u, moraju da bude autentifikovani. Autentifikacija se vrši preko Windows autentifikacionog protokola. Između njih se otvara siguran komunikacioni kanal, tako da treća strana neće moći da pristupi podacima koji se šalju.

```
Connection with MS servis is succesfull.  
Korisnik koji je pokrenuo klijenta je : DESKTOP-AV2PARO\Engineer1  
  
1: Procitaj konfiguraciju  
2: Dodaj proces  
3: Izmeni parametre konfiguracije  
4: Izbrisi proces  
5: Izbrisi konfiguracioni fajl  
6: Završi rad programa
```

Da bi mogao da izmeni konfiguraciju klijent prvo mora biti autorizovan za to radnju i to se postiže RBAC modelom. RBAC (Role-Based Access Control) je tip autorizacije kojim se svakom korisniku dodeljuje jedna od definisanih uloga, a svakoj ulozi jedna ili više dozvola. Na taj način MS proverava kojoj ulozi pripada klijent i da li ta uloga ima dozvolu za traženu radnju.

Postoje 4 uloge i ukupno 5 radnji nad konfiguracijom: Manager može da pročita konfiguraciju ali nema pravo da napravi izmenu; Engineer ima pravo da izmeni postojeće parametre u konfiguraciji, kao i da dodaje nove procese, ali nema pravo da briše postojeće procese; Support Member ima pravo da izmeni postojeće parametre u konfiguraciji, da dodaje nove procese kao i da briše postojeće; Chief Officer jedina grupa korisnika koja ima pravo da obriše konfiguracioni fajl.

```
C:\Users\Administrator\Documents\OIBIS-Test\OIBISProjekat\Client\bin\Debug\Client.exe  
izmenaProcesa  
  
1: Procitaj konfiguraciju  
2: Dodaj proces  
3: Izmeni parametre konfiguracije  
4: Izbrisi proces  
5: Izbrisi konfiguracioni fajl  
6: Završi rad programa  
4  
Unesi proces za brisanje: noviProces  
User Engineer1 try to call DeleteProcess method. DeleteProcess method need DeleteProcess permission.
```

```
3: Izmeni parametre konfiguracije
4: Izbrisi proces
5: Izbrisi konfiguracioni fajl
6: Zavrshi rad programa
1
git-bash
wsappx
bash
testProces

1: Procitaj konfiguraciju
2: Dodaj proces
3: Izmeni parametre konfiguracije
4: Izbrisi proces
5: Izbrisi konfiguracioni fajl
6: Zavrshi rad programa
2
Unesi proces: noviProces
Proces dodat

1: Procitaj konfiguraciju
2: Dodaj proces
3: Izmeni parametre konfiguracije
4: Izbrisi proces
5: Izbrisi konfiguracioni fajl
6: Zavrshi rad programa
1
git-bash
wsappx
bash
testProces
noviProces
```

Zaključak

Malware Scanning system bi se mogao koristiti bi se mogao koristiti kao zaštita od zlonamernog softvera. Potencijalno značajno unapređenje bilo bi sakupljanje veće baze nedozvoljenih procesa koji bi se na primer dobavljali iz neke poznatije baze sličnih sistema.