IBIS Documentation

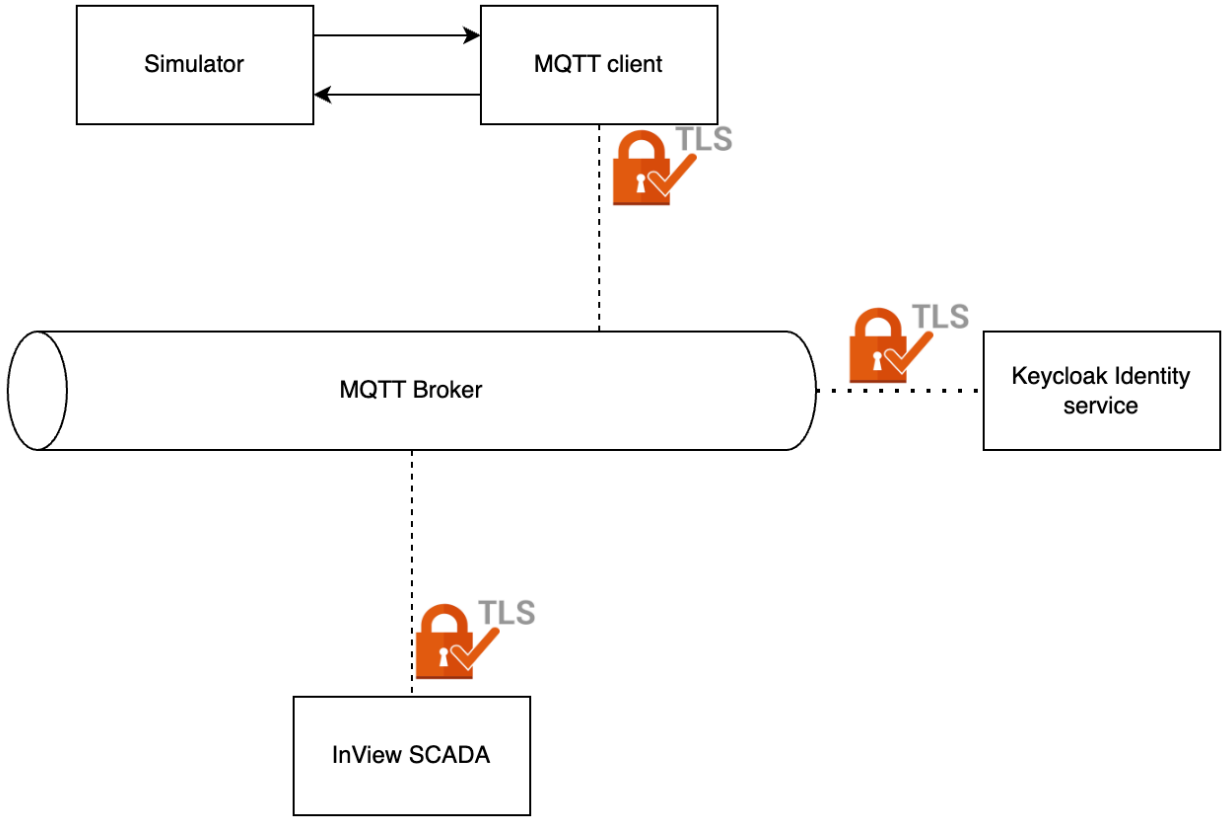
Github source code repo: https://github.com/markopex/IBIS_Project

Marko Đorđić, Marko Đurđević

Uvod

U okviru ovog projekta urađena je nadogradnja proslogodišnjeg projekta Metro (https://github.com/Djordje99/IBIS_Project). Arhitektura sistema je unapređena u pravcu povećanja bezbednosti sistema. To je postignuto dodavanjem servisa za autentifikaciju i autorizaciju korisnika kao i obezbeđivanjem komunikacionih kanala.

Svi komunikacioni kanali sada su zaštićeni enkripcijom, zahvaljujući dodatim TLS sertifikata. Sertifikati su generisani putem Let's Encrypt sajta i vezani su za domen cybergym.space, što eliminiše mogućnost napada sniffing-om, jer sadržaj poruka nije moguće pročitati.



Slika 1. Arhitektura unapređenog sistema

U narednim poglavljima redom će biti objašnjeni elementi projekta, Simulator i MQTT Client, zatim kratko opisana InView SCADA i rukovanje sistemom, kao i jedan scenario napada na ovaj sistem.

1. Keycloak Identity Servis

Keycloak je dodan kao centralni servis za autentifikaciju i autorizaciju korisnika. Keycloak pruža sveobuhvatne mogućnosti upravljanja identitetima, uključujući podršku za RBAC (Role-Based Access Control). Ovaj servis omogućava definisanje različitih uloga korisnika i prava pristupa, čime se osigurava da samo ovlašćeni korisnici mogu pristupiti određenim resursima i funkcionalnostima sistema. Keycloak se integriše sa Mosquitto MQTT brokerom putem OAuth plugina, omogućavajući bezbednu autentifikaciju i autorizaciju korisnika koji pristupaju MQTT brokeru.

2. Mosquitto MQTT Broker

Mosquitto MQTT broker je nadograđen dodavanjem OAuth plugina, što omogućava integraciju sa Keycloak servisom za autentifikaciju i autorizaciju. Ova nadogradnja omogućava da se u Keycloak-u definišu topici kojima korisnici mogu pristupiti, osiguravajući da samo ovlašćeni korisnici mogu videti i upravljati određenim podacima. Svi komunikacioni kanali između MQTT client-a i brokera sada su zaštićeni TLS enkripcijom, čime se eliminišu napadi sniffing-om i osigurava bezbedan prenos podataka.

3. Simulator

Simulator je kreiran kao Flask REST API aplikacija. U modulu Api nalaze se svi pozivi REST API-a koje je moguće pozvati, i oni su raspoređeni u posebne module koje su objedinjeni uz pomoć blueprint-a. Modul Model sadrži modele voza i pruge koji će biti potrebni simulatoru za obradu. Konačno, sam Simulator.py sadrži čitavu logiku koju simulator izvršava. Rešenje koje je implementirano sadrži tri niti koje se pokreću istovremeno i koje predstavljaju vozove (kako imamo tri trase metroa, tako imamo i tri voza). Sve tri niti se oslanjaju na threading.Event koji služi da se niti zaustave na zahtev i nastave sa radom od prethodno zaustavljenog položaja.

4. MQTT Client

Zadatak MQTT client-a je da očitava podatke sa Simulator-a i objavljuje ih na MQTT broker. Pored osluškivanja izmena na Simulator-u, takođe je neophodno biti subscribe-ovan na topike koji se menjaju na SCADA-i i obaveštavati simulator o njihovim izmenama. MQTT client sada koristi TLS enkripciju za bezbednu komunikaciju sa MQTT brokerom. Aplikacija je kreirana kao Flask REST API i oslanja se na multiprocess dizajn, tako da se pokretanjem pokreće više procesa:

1. Ažuriranje stanja metroa odnosno prelaza
2. Ažuriranje stanja voza na trasi A
3. Ažuriranje stanja voza na trasi B
4. Ažuriranje stanja voza na trasi C
5. Osluškivanje upravljanja sa SCADA-e

5. InView SCADA

InView Cloud SCADA rešenje omogućava daljinsko nadgledanje i upravljanje kao i prikupljanje podataka i to samo pomoću pretraživača. Dva glavna dela u okviru ovog sistema su Editor i Client. U okviru Editora se vrše podešavanja kao i generisanje prikaza koje će se kasnije prikazivati i menjati na Client-u. Da bi SCADA imala mogućnost prikupljanja podataka neophodno je u okviru Editora definisati sledeće elemente:

1. Connections - definiše konekciju ka MQTT broker-u sa kog će se osluškivati topic-i, odnosno variable u InView, kao i slati promene tih varijabli
2. Devices - u okviru kog je neophodno definisati jedan uređaj
3. Variables - definiše varijable (ime varijable, tip, …)

Scenario napada na sistem

U ovom scenariju sajber napada, napadač koristi tehniku phishinga kako bi preuzeo kontrolu nad računarom ciljanog korisnika. Napad se izvodi sledećim koracima:

1. **Priprema Phishing Emaila:**
   Napadač kreira lažni email sa temom "Secret Santa", koji se šalje zaposlenima unutar organizacije. Email je dizajniran da izgleda kao da dolazi od pouzdanog izvora, na primer, od HR tima ili od menadžera. Priprema malicioznog emaila je ključni deo napada, jer je potrebno da izgleda dovoljno verodostojno da bi žrtva poverovala u njegovu autentičnost. Secret Santa predstavlja jedan od korektnih primera jer nije može proći neopaženo naravno kad se slanje tempira na period oko Nove godine.

Primer Emaila:

```
Od: HR Team <hr@metroscada.com>
Predmet: Secret Santa - Učestvujte u našem prazničnom darivanju!

Dragi zaposleni,

Sezona praznika je pred nama, i vreme je za našu tradicionalnu igru Secret Santa!
Da biste učestvovali, molimo vas da popunite priloženi dokument i napišete svoje želje
Deda Mrazu.

Radujemo se vašem učešću i želimo vam srećne praznike!

Srdačan pozdrav,
HR Team
```

2. **Priloženi Maliciozni Dokument:**
   Email sadrži priloženi DOCX fajl nazvan "SecretSanta.docx". Kada zaposleni otvori ovaj dokument, prikazan mu je formular gde treba da napiše svoje želje Deda Mrazu. Dokument izgleda bezopasno, ali sadrži ugrađeni maliciozni makro.

3. **Maliciozni Makro:**
Unutar DOCX fajla se nalazi makro koji se automatski pokreće kada korisnik klikne na opciju za editovanje dokumenta. Ovaj makro je dizajniran da uspostavi "reverse shell" konekciju ka napadaču.

Opis Makra:
- Kada se dokument otvori i korisnik klikne na "Enable Editing" ili "Enable Content", makro se aktivira.
- Makro preuzima i pokreće skriptu koja uspostavlja povratnu konekciju (reverse shell) sa napadačem.
- Kroz reverse shell, napadač dobija pristup komandnoj liniji zaraženog računara i može da izvršava komande sa daljine.

4. **Preuzimanje Kontrole:**
- Napadač sada ima kontrolu nad računarom ciljanog korisnika. Može pregledati fajlove, instalirati dodatni malver, eksfiltrirati poverljive informacije ili koristiti računar kao odskočnu dasku za dalje napade unutar mreže organizacije.