Fakultet tehničkih nauka, Univerzitet u Novom Sadu

Predmet: Informaciona bezbednost u infrastrukturnim sistemima (IBIS)

Tema projekta: Bezbednost računarskih mreža u KI

Student: Nikola Miljković

Datum: Oktobar 2025

## 1. Uvod

Cilj ovog projekta je simulacija komunikacije u industrijskim kontrolnim sistemima (ICS) koristeći Modbus TCP/IP protokol, analiza mrežnog saobraćaja i implementacija bezbednosnog sloja putem proxy servera. Projekat je povezan sa predmetom IBIS jer omogućava razumevanje kritičnih infrastrukturnih sistema, SCADA arhitektura, analize rizika i sajber incidenta.

## 2. Opis projekta

Projekat se sastoji od tri glavne komponente:

1. 1. **Modbus server**: simulira senzore i aktuatora industrijskog sistema.
2. 2. **Proxy sloj**: presreće i analizira saobraćaj, omogućava filtriranje i bezbednosnu kontrolu.
3. 3. **Client (UI)**: web interfejs za vizualizaciju podataka i upravljanje sistemom.

Tehnologije korišćene u projektu:

* - Python (server, proxy, client)
* - Flask (web interfejs)
* - Docker i Docker Compose (kontenerizacija)
* - Wireshark (analiza saobraćaja)
* - MQTT (opciono za komunikaciju sa SCADA HMI)

## 3. Protokoli i komunikacija

* **Modbus TCP/IP**: osnovni protokol za komunikaciju između servera i klijenta. Omogućava čitanje i pisanje registara senzora i aktuatora.
* **HTTP/Flask**: web interfejs za kontrolu i vizualizaciju podataka.
* **Proxy sloj**: presreće sve Modbus poruke, omogućava filtriranje i potencijalno logovanje saobraćaja za analizu.

## 4. Implementacija

### 4.1 Modbus server

Server implementira set registara koji predstavljaju senzore i aktuatora. Komande se obrađuju u realnom vremenu.

# Primer pseudokoda servera  
from pyModbusTCP.server import ModbusServer  
server = ModbusServer(host="0.0.0.0", port=502, no\_block=True)  
server.start()

### 4.2 Proxy sloj

Proxy presreće komunikaciju između servera i klijenta, proverava ispravnost komandi i loguje aktivnosti.

# Pseudokod proxy-a  
while True:  
 data = read\_from\_client()  
 if valid(data):  
 forward\_to\_server(data)

### 4.3 Client / UI

Flask web aplikacija prikazuje podatke u realnom vremenu i omogućava korisniku da šalje komande.

from flask import Flask, render\_template  
app = Flask(\_\_name\_\_)  
@app.route('/')  
def index():  
 return render\_template('index.html')

### 4.4 Docker Compose

version: '3'  
services:  
 modbus\_server:  
 build: ./server  
 ports:  
 - "502:502"  
 proxy:  
 build: ./proxy  
 ports:  
 - "1502:502"  
 client\_ui:  
 build: ./client  
 ports:  
 - "8080:8080"

### 4.5 Pokretanje i testiranje

* run\_local.sh i stop\_local.sh skripte omogućavaju start/stop lokalnog okruženja.
* run\_with\_ui.sh omogućava pokretanje sa web interfejsom.
* Wireshark se koristi za proveru TCP/UDP paketa i potvrdu ispravne komunikacije.

## 5. Analiza bezbednosti i rizika

* **MITM napadi**: Proxy sloj omogućava simulaciju i zaštitu od presretanja paketa.
* **Replay napadi**: Evidentiranje komandi i vremenskih oznaka smanjuje rizik.
* **Logovanje saobraćaja**: Wireshark analize omogućavaju detekciju anomalija.
* **Portovi**: 502 (Modbus TCP), 8080 (HTTP UI).

## 6. Zaključak i budući rad

Projekat omogućava razumevanje ICS sistema i njihovih sajber rizika. Buduće proširenje može uključivati autentifikaciju, enkripciju Modbus poruka, integraciju sa stvarnim SCADA HMI sistemom i detaljniju simulaciju napada.

## 7. Literatura

1. Pascal Ackerman, *Industrial Cybersecurity – Efficiently secure critical infrastructure systems*, Packt, 2017.
2. George Loukas, *Cyber-Physical Attacks: A Growing Invisible Threat*, Butterworth-Heinemann, 2015.
3. Clint Bodungen, Bryan Singer, Aaron Shbeeb, Kyle Wilhoit, Stephen Hilt, *Hacking Exposed Industrial Control Systems*, McGraw-Hill Education, 2016.
4. Knapp E.D., *Industrial network security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*, 2011.
5. Materijali sa predmeta IBIS 2024, Fakultet tehničkih nauka, UNS.
6. Vlastiti kod i dokumentacija projekta.