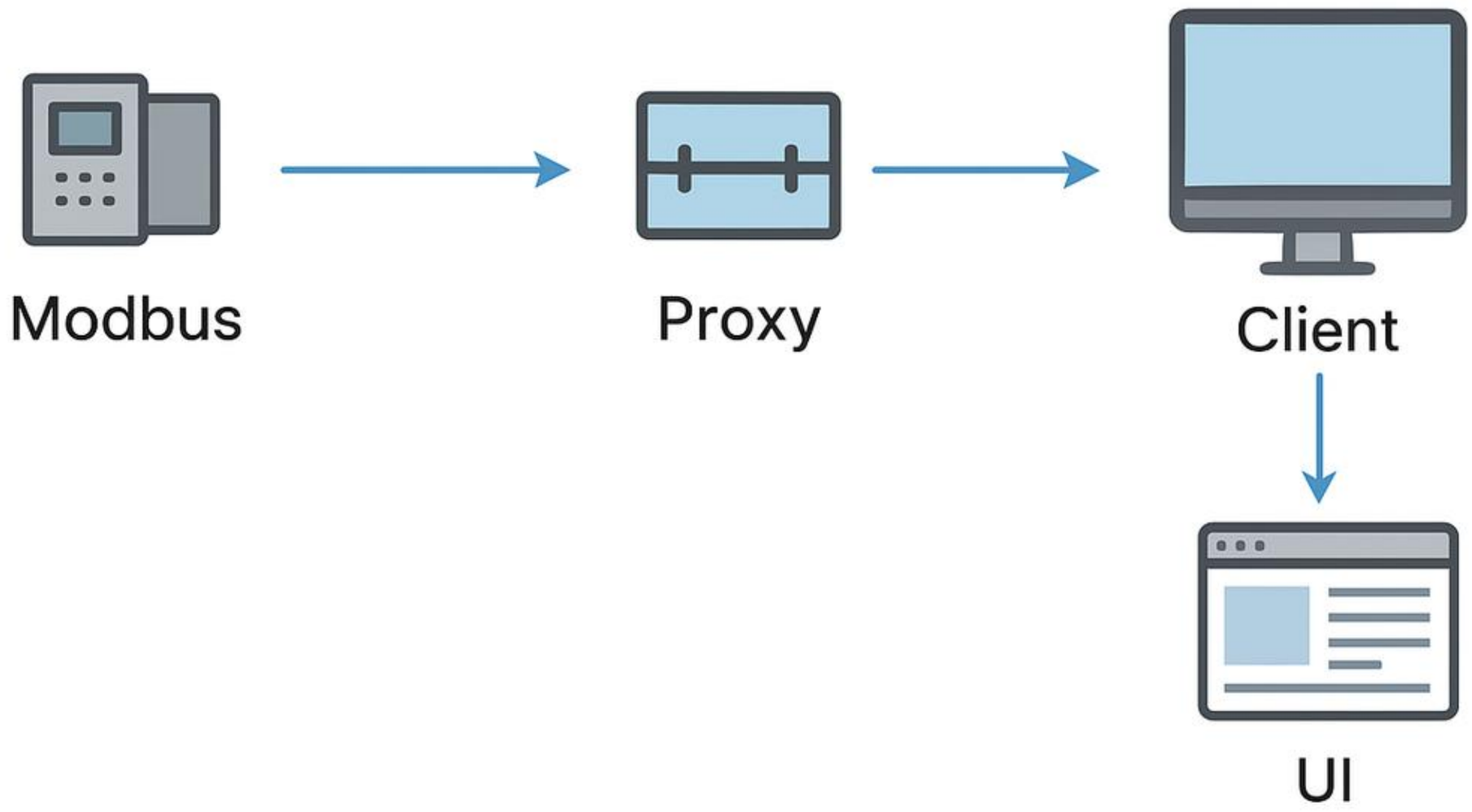
IBIS — Demo: Modbus MITM Simulator (proxy) — Sažetak



Cilj projekta: edukativna demonstracija Man-in-the-Middle (MITM) simulacije nad Modbus TCP sistemom koristeći eksplicitni proxy.

Sadržaj slike: dijagram toka + detaljan opis kako sistem radi i koje protokole koristi.

Arhitektura:
- modbus_server: simulator PLC-a (piše vrednost u holding reg 0)
- modbus_proxy: eksplicitni proxy koji čita sa servera, opcionalno manipuliše registarom i izlaže podatke HMI-ju
- modbus_client (HMI): čita vrednost preko proxy-ja
- ui_server (Flask): web UI koji prikazuje vrednost i omogućava uključivanje/isključivanje manipulacije

Kako radi:
1) Server upisuje nasumičnu temperaturu u holding register 0 (Modbus TCP).
2) Proxy periodično čita registre sa servera i postavlja ih u internu DataBank.
   - Ako je manipulacija uključena (control.json), proxy menja reg0: +10.
3) Klijent/HMI čita reg0 sa proxy-ja i prikazuje (može biti 'manipulisano').
4) UI omogućava kontrolu (on/off) preko control.json i direktno upisivanje vrednosti koristeći manipulator skriptu.

Korišćeni protokoli/tehnologije:
- Modbus TCP (aplikacioni protokol za industrijske uređaje) — transport: TCP/IP
- HTTP (Flask UI) za nadzor i kontrolu preko pregledača
- Lokalni fajl (control.json) za dinamičnu kontrolu manipulacije
- Python (pyModbusTCP, Flask, scapy za defense monitor)

Šta se dešava pri simulaciji napada (MITM simulacija):
- Napad nije na nivou ARP spoofinga; umesto toga koristi se eksplicitni proxy koji preusmerava i manipuliše podatke.
- Proxy funkcionše kao posrednik: HMI -> Proxy -> Server. Proxy može menjati vrednosti pre nego što ih HMI vidi.

Poenta projekta:
- Edukacija: pokazuje kako MITM može uticati na SCADA/ICS podatke bez brutalnog narušavanja fizičke mreže.
- Siguran testbed: bez ARP-spoofinga, sa jasnom kontrolom manipulacije kroz UI.
- Demonstrira zasnovane odbrane: detekcija anomalija (defense_module).