Model pretnji IOT sistema

I. Tokovi podataka analiziranog modula:

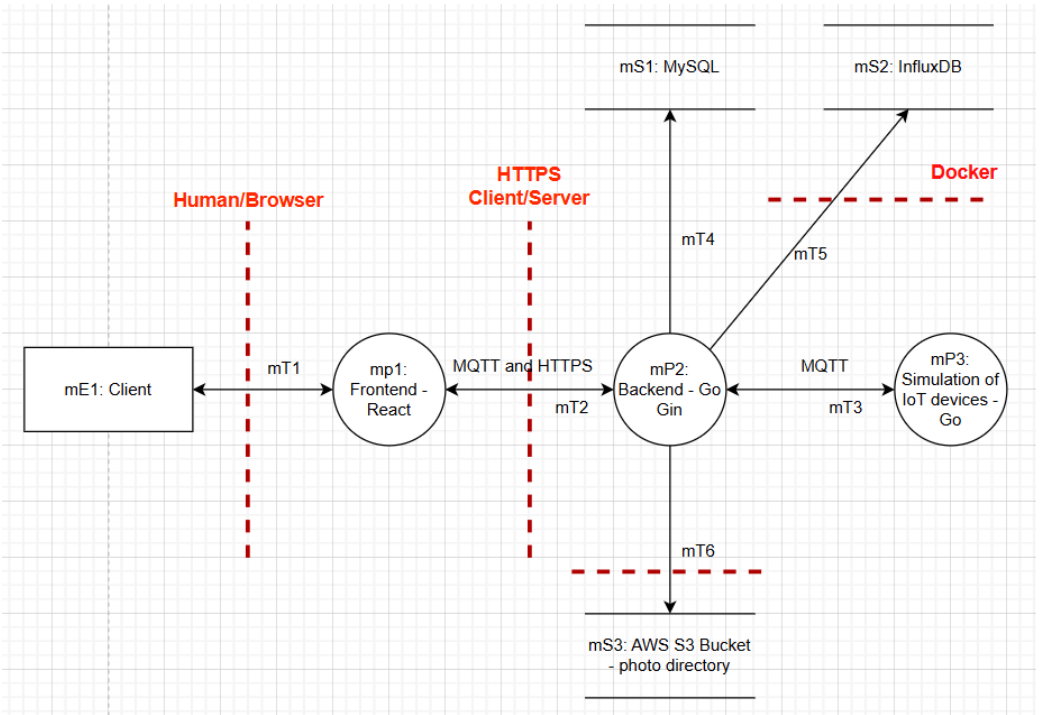
Analiziran modul predstavlja aplikaciju za podršku Smart Home pametnih uređaja. Aplikacija pruža sljedeće funkcionalnosti:

- registrovanje nekretnina
- registrovanje pametnih uređaja
- upravljanje pametnim uređajima
- pregled trenutnog stanja uređaja
- dodavanje člana porodice

Softver se sastoji od:

- klijentske aplikacije, izrađene u *React* tehnologiji
- serverske aplikacije, izrađene u *Go Gin* radnom okviru
- aplikacije koja simulira rad uređaja, pisane u *Go* programskom jeziku
- *MySQL* baze podataka
- AWS S3 *bucket* servisa u svrhu skladištenja fotografija
- *InfluxDB* baze u svrhu skladištenja *timeseries* podataka (podaci iz simulacije koji imaju vremensku odrednicu kada je mjerenje izvršeno)

Dijagram ispod prikazuje za analiziran modul (m) procesne komponente (mP), skladišta (mS), tokove podataka (mT) i eksterne entitete (mE).



II. Resursi i pretnje visokog nivoa:

1. Manipulacija podacima u realnom vremenu i napad na IoT uređaje

1. Napad na IoT uređaje
   ├── 1.1 Otmica IoT uređaja
   │   ├── 1.1.1 Zloupotreba slabih lozinki ili nezaštićenih autentifikacionih mehanizama
   │   ├── 1.1.2 Napad na mrežni sloj (npr. Man-in-the-Middle napad)
   │   └── 1.1.3 Exploitacija ranjivosti u firmware-u uređaja
   ├── 1.2 Napadi na komunikaciju između uređaja
   │   ├── 1.2.1 Sniffing (presretanje) podataka u tranzitu
   │   └── 1.2.2 Manipulacija paketima (npr. replay attack)
   └── 1.3 Napadi na backend servis (oblak) koji prikuplja podatke
       ├── 1.3.1 SQL injection u sistemu za analizu podataka
       └── 1.3.2 Napad na API-je koji prikupljaju podatke od IoT uređaja

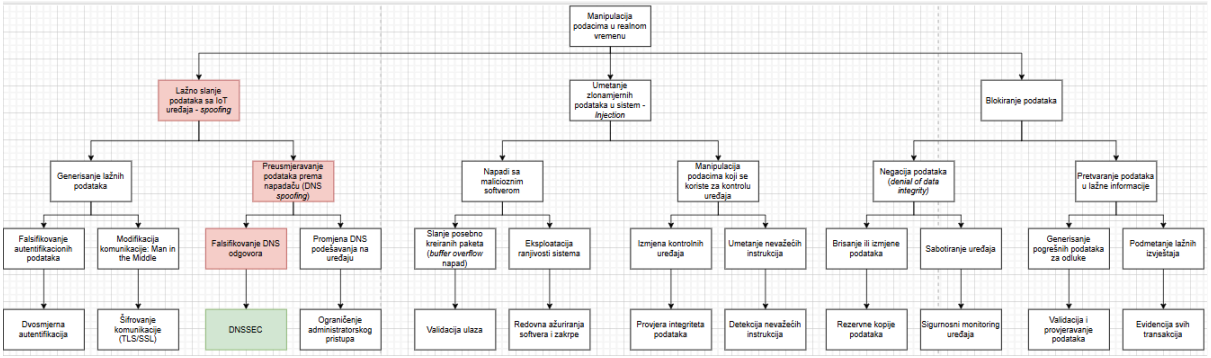
2. Manipulacija podacima u realnom vremenu
   ├── 2.1 Lažno slanje podataka sa IoT uređaja
   │   ├── 2.1.1 Generisanje lažnih podataka (falsifikovanje senzornih vrednosti)
   │   └── 2.1.2 Preusmeravanje podataka prema napadaču (npr. DNS spoofing)
   ├── 2.2 Umetanje zlonamernih podataka u sistem
   │   ├── 2.2.1 Napadi sa malicioznim paketima (npr. buffer overflow napadi)
   │   └── 2.2.2 Manipulacija podacima koji se koriste za kontrolu uređaja
   └── 2.3 Distorzija ili blokiranje podataka
       ├── 2.3.1 Negacija podataka (denial of data integrity)
       └── 2.3.2 Pretvaranje podataka u lažne informacije (npr. proizvodnja pogrešnih podataka za odluke)

3. Napadi na kontrolu uređaja
   ├── 3.1 Preuzimanje kontrole nad uređajem
   │   ├── 3.1.1 Zloupotreba administratorskog pristupa uređaju
   │   ├── 3.1.2 Korišćenje ranjivosti u operativnom sistemu uređaja
   │   └── 3.1.3 Korišćenje povlastica na mreži za preuzimanje kontrole (privilegije povišene na uređajima)
   └── 3.2 Onemogućavanje uređaja (DoS napad)
       ├── 3.2.1 Preopterećenje uređaja sa zahtevima
       └── 3.2.2 Korišćenje botnet mreže za napad na uređaje

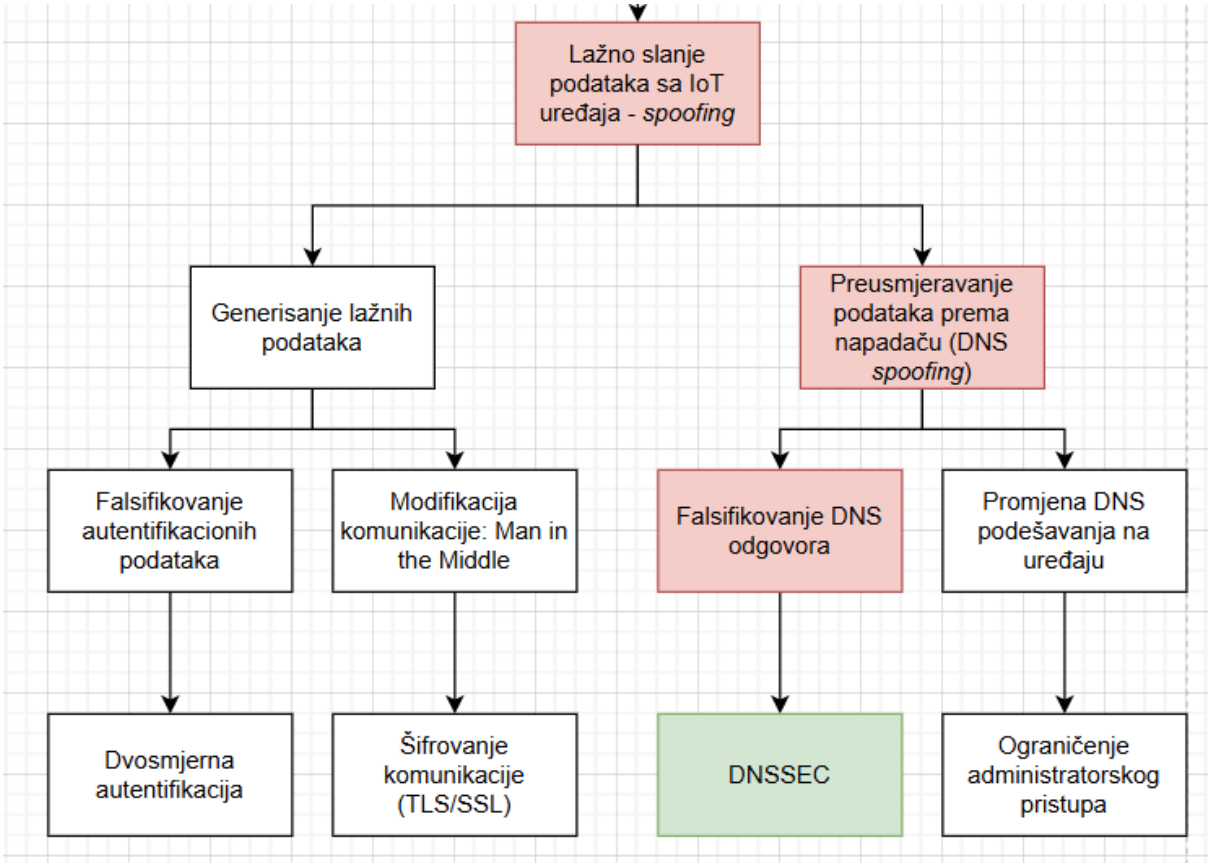
4. Odbrana od napada
   ├── 4.1 Ojačavanje autentifikacije
   │   ├── 4.1.1 Korišćenje jakih lozinki i dvofaktorske autentifikacije (2FA)
   │   └── 4.1.2 Implementacija TLS/SSL za autentifikaciju uređaja
   ├── 4.2 Sigurnost komunikacije
   │   ├── 4.2.1 Šifrovanje podataka u tranzitu (npr. SSL/TLS)
   │   └── 4.2.2 Verifikacija integriteta podataka (npr. HMAC ili digitalni potpisi)

- 4.3 Praćenje i detekcija anomalija
  - 4.3.1 Uvođenje sistema za detekciju napada (IDS/IPS)
  - 4.3.2 Praćenje svih komunikacija između uređaja i backend-a
- 4.4 Sigurnost firmware-a
  - 4.4.1 Redovno ažuriranje firmware-a i zakrpe za uređaje
  - 4.4.2 Verifikacija autentičnosti firmware-a (npr. digitalni potpisi)
- 4.5 Sigurnost backend servisa
  - 4.5.1 Korišćenje API rate limiting i autentifikacije za pristup podacima
  - 4.5.2 Sigurnost baza podataka sa enkripcijom i pravilima pristupa

Stablo za prijetnju 1 napad 2 - manipulacija podacima u realnom vremenu



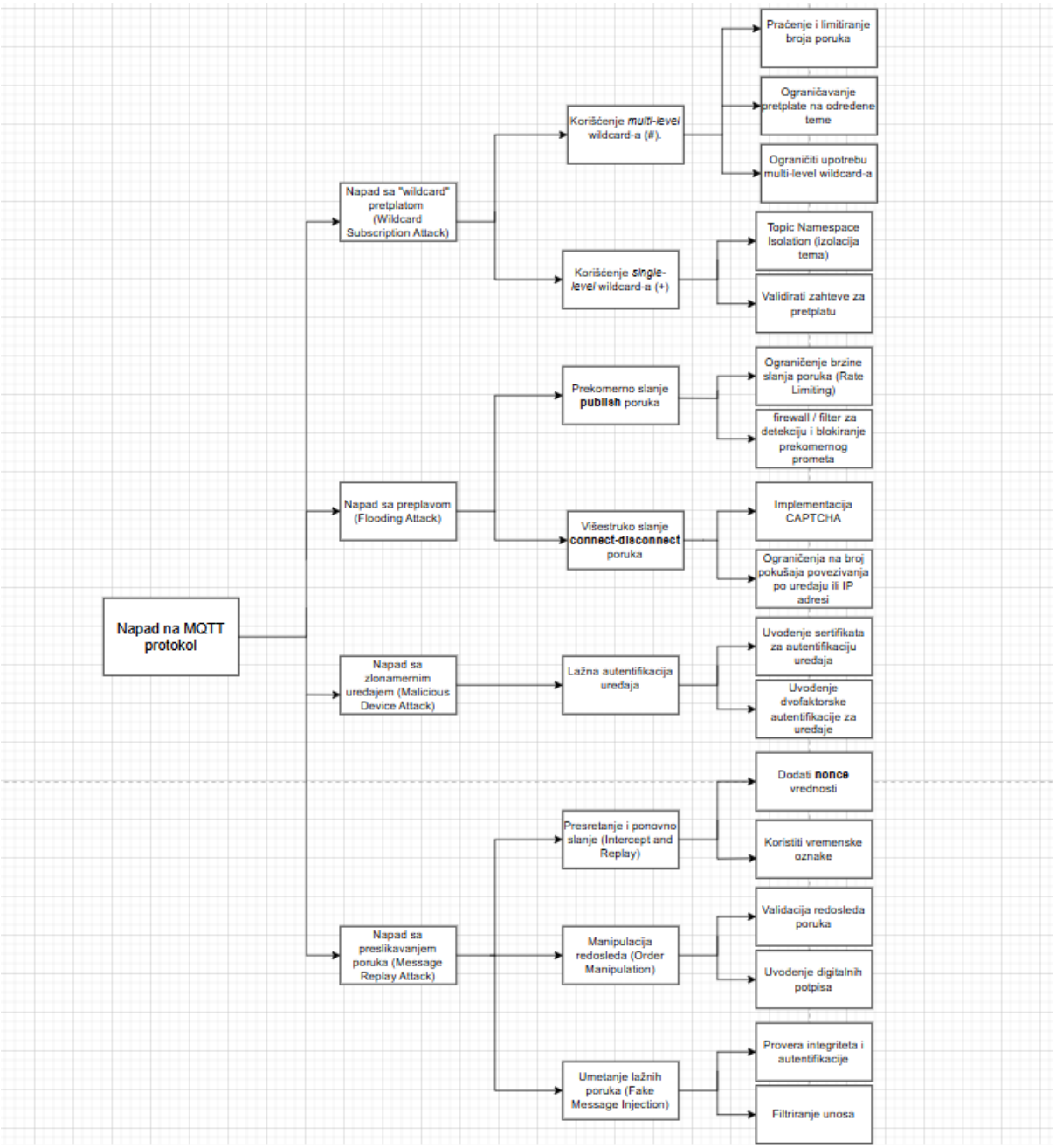
U daljem tekstu će detaljno biti analiziran DNS *spoofing* napad, konkretno za uređaj pametna kapija.



teze:

- objasniti šta je dns spoofing
- kako se radi
- dati primjer koda
- objasniti na konkretnom primjeru pametne kapije šta i zašto će se zloupotrijebiti
- objasniti kako uraditi mitigaciju (DNSSEC)

2. Napad na sigurnosni protokol MQTT



III. Dubinska analiza napada i mitigacija

A. DNS *spoofing*

DNS (*Domain Name Server*) *spoofing* će biti objašnjen na primjeru iskorištavanja informacija o pametnoj kapiji.

DNS *spoofing* napad podmeće lažnu ip adresu na koju preusmjerava sve DNS zahtjeve. U kontekstu pametne kapije, može da dobija informacije kada je kapija otvorena i da šalje lažnu informaciju o trenutnom stanju kapije na *frontend*.

Podmetanje lažnog MQTT brokera je jedan od načina da se realizuje ovaj napad.