**Kauno technologijos universitetas**

Informatikos fakultetas

Taikomosios informatikos katedra

**Programų sistemų inžinerija**

**p175B015**

**Application Layer (L7) Firewall component**

**HRPI analyzer**

Atliko ELITNET1:

Robertas Strazdauskas, IFF-6/7

Kazimieras Buškus, IFF-6/9

Šarūnas Andrijauskas, IFF-6/7

Tomas Jurevič, IFF-6/1

Priėmė:

Andrej Ušaniov

# Projekto tikslas

Sukurti taikomųjų programų lygio (7-o OSI architektūros lygio) ugniasienės komponentą, kuris pateiktų efektyvią, realiu laiku galinčią veikti sistemos struktūrą bei sąveikaujančias apdorojimo funkcijas. Analizatorius taip pat pateikia sistemos administratoriams paprastą naudoti grafinę sąsają tinklo srauto stebėjimui.

Pagrindinės ugniasienės komponento atliekamos funkcijos:

1. Programų lygio DDoS atakų aptikimas. Šis sprendimas turi aptikti tinklo pralaidumą ir serverio resursus švaistančias HTTP GET užklausų atakas, remdamasis tam tikromis statistinėmis atakų savybėmis.
2. Būsenos stebėjimas. Analizatorius teikia intuityvias tinklo srauto stebėjimo galimybes, atakos įspėjimo sistemą, ankstesnių būsenų grafikus ir manipuliacijas su istoriniais duomenimis.

# Užduoties analize: techninis pasiūlymas

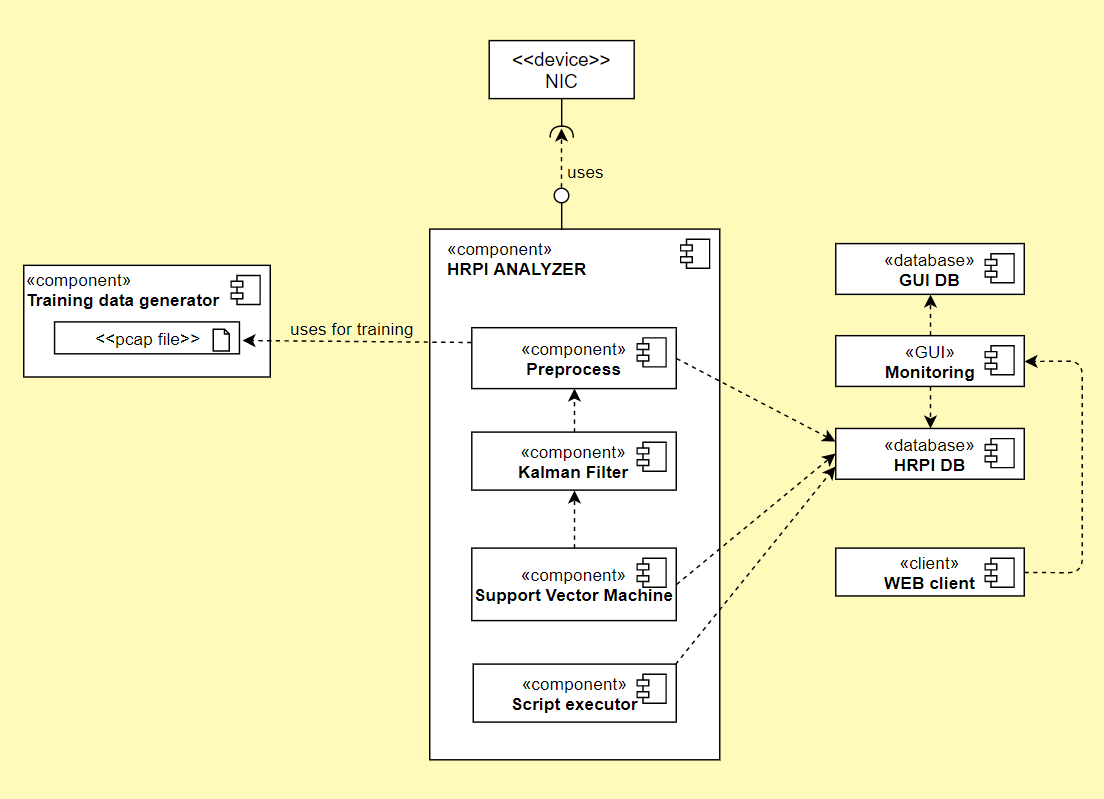
1. **Apibrėžimai bei sutrumpinimai:**
   1. HTTP – HyperText Transfer Protocol
   2. TCP– Transfer Control Protocol
   3. SVM –Support Vector Machine
   4. HRPI – HTTP GET Requests Per IP
   5. DDoS –Distributed Denial of Service
   6. API –Application Programming Interface
2. **Sprendimo apžvalga**

HRPI analizavimo modulis aptinka programos lygio DDoS atakas ir veikia kaip vienas iš L7 lygio ugniasienės komponentų.

Naudojant matematinį metodą[[1]](#footnote-1), ši programa gali efektyviai aptikti atakas ir paleisti atitinkamų veiksmų rinkinį. Sprendimas taip pat pateikia lengvai naudojamą grafinę naudotojo aplinką su programos duomenų srauto stebėjimo bei atakos pranešimais. Grafinė vartotojo sąsaja taip pat gali pateikti istorinius duomenis.

Šis sprendimas susideda iš apmokymo duomenų kūrimo SVM apmokymui aptikti atakas, bei jos testavimui.

1. **Komponentų apžvalga**

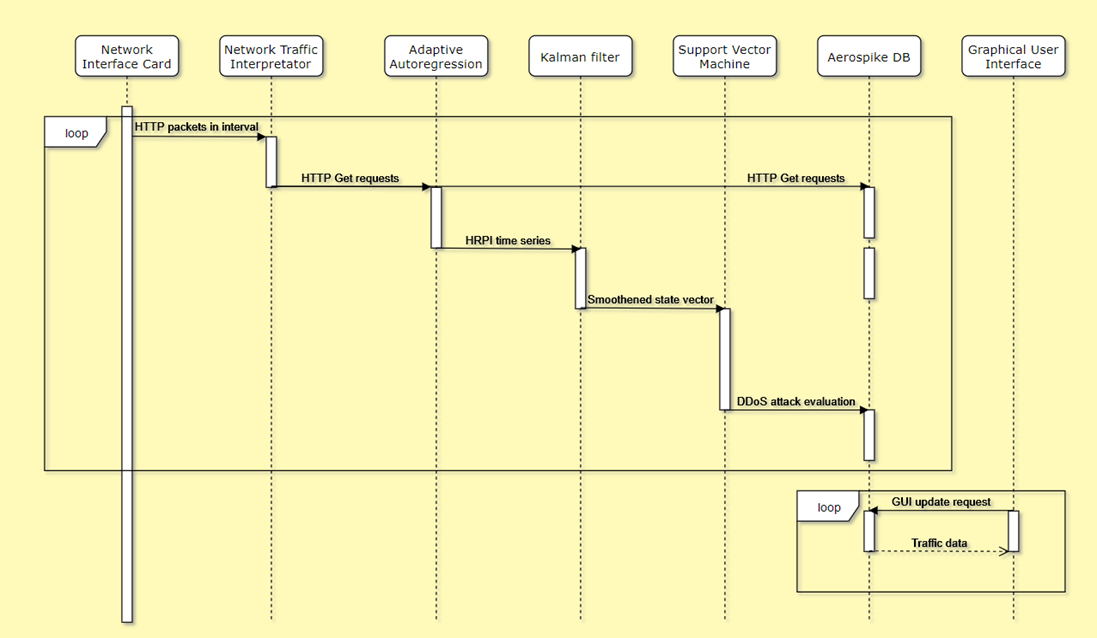


1 pav. Komponentų schema

* NIC – Network Interface Card – prietaisas su kuriuo modulis tiesiogiai bendrauja, kad gautų realaus laiko duomenų srauto duomenis
* Training data generator – programa atsakinga už apmokymo duomenų generavimą SVM klasifikatoriui
* Preprocess – algoritmas skirtas paversti paketinius duomenis iš NIC į HRPI, kurie bus naudojami matematinio modelio
* Kalman filter – algoritmas skirtas įvertinti esamą duomenų srauto būseną
* Support Vector Machine – algoritmas skirtas atskirti atakos duomenų srautą nuo įprasto srauto
* Monitoring –Grafinė vartotojo sąsaja WEB, skirta stebėti esamą srautą ir istorinius duomenis
* Script executor – programa atakos atveju paleidžianti iš anksto numatytą programą.
* GUI DB – Maria DB skirta saugoti GUI informacija, pavyzdžiui prisijungimo informaciją.
* HRPI DB – Aerospike DB skirta realaus laiko duomenų srauto informacijai saugoti
* WEB client – programa veikianti naudotojo naršyklėje

1. **Sąsajos apžvalga**
   1. WIRE – TCP pagrįstas protokolas skirtas bendrauti su Aerospyke duomenų baze
   2. HTTP interface – HTTP protokolas naudojamas bendravimui tarp GUI ir WEB kliento
   3. SQLCNTR – SQL jungties sutrumpinimas – standartinis Python API bendravimui su MariaDB
2. **Veikimo apžvalga**

Vieno laiko intervalo paketų rinkinio įvertinimo vykdymo sekos diagrama:

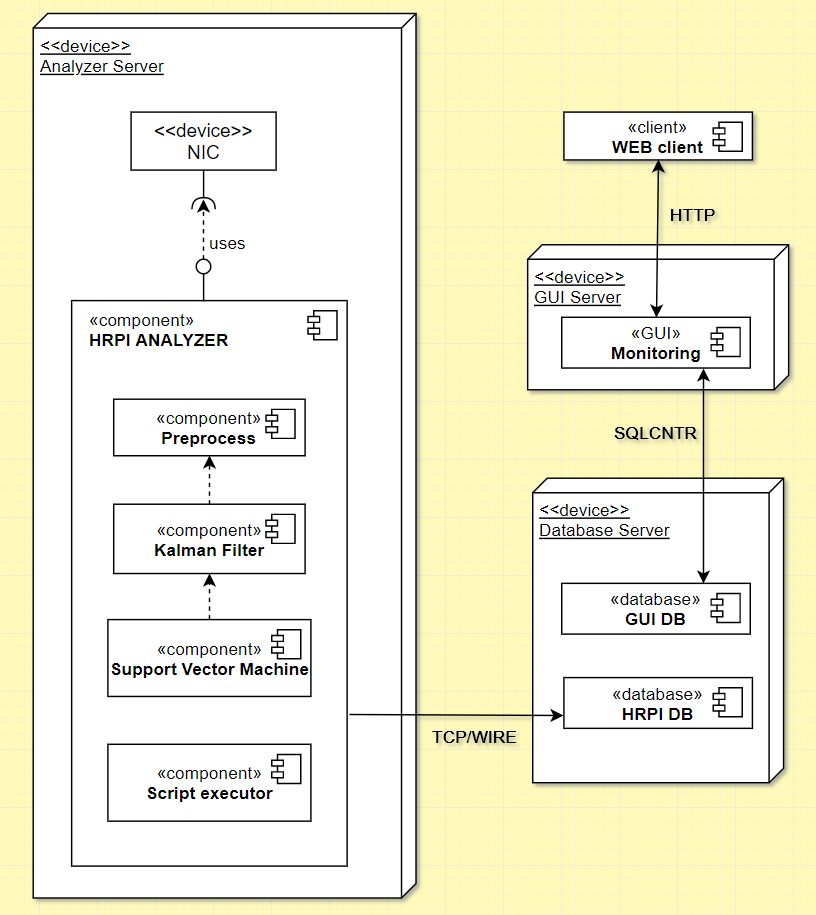


2 pav. Vieno laiko intervalo paketų rinkinio įvertinimo vykdymo sekos diagrama

1. **Pavojaus įspėjimas ir stebėjimas**

Pavojaus įspėjimas yra pateikiamas grafine sąsaja. Programa įrašo duomenų srautą ir jo klasifikavimą, todėl grafikai yra pažymimi atitinkamomis spalvomis.

1. **Įdiegimo rodinys**



3 pav. Įdiegimo rodinio schema

# Įvardinti projekto funkciniai ir nefunkciniai reikalavimai

1. **Funkciniai reikalavimai**
   1. **Bendri reikalavimai**

FBR-1 Šis sprendimas turi suteikti galimybę paleisti iš anksto nustatytus veiksmus / programas pagal esamą duomenų srautą.

FBR-2 Modulis turi palaikyti aukštą pasiekiamumą: programa bus paleista dvejuose mazguose vienu metu.

FBR-3 Modulis turi palaikyti statistikos stebėjimą:

1. Peržiūrėti dabartinę ir istorinę užklausų peržiūrą
2. Peržiūrėti dabartinę ir istorinę duomenų srauto informaciją atakos metu
3. Išpuolio metu pateikti aktyviausių mazgų peržiūrą

FBR-4 Metrikos turi būti prieinamos per interneto GUI

FBR-5 Metrikos istorinis kontekstas turi įtraukti grafiko laiko matavimo vienetus: minutes, valandas, dienas

FBR-6 Modulis turi palaikyti prisijungimo sistemą

FBR-7 Šis sprendimas turi naudoti didelio efektyvumo skaičiavimo metodus ir apdoroti 1Gb duomenų per sekundę.

* 1. **Serverio reikalavimai**

FSR-1 Serveris turi pateikti GUI prieigą per internetą

FSR-2 MariaDB duomenų bazė turi laikyti: GUI indentifikavimo informaciją

FSR-3 Aerospyke duomenų bazė turi saugoti periodinę duomenų tinklo srauto ir klasifikavimo informaciją.

* 1. **Kliento pusės reikalavimai**

FKR-1 Prisijungimas naudojantis vartotojo vardą ir slaptažodį

FKR-2 Atsijungimo nuo kliento funkcija

FKR-3 Realaus laiko tinklo srauto metrinė grafika

FKR-4 Įtartinos veiklos, atakų statistikos metrika

* + 1. **GUI reikalaviami**

FKR-5 Realiu laiku atnaujinamos, lengvai suprantamos diagramos, kurios turi įtraukti:

1. HRPI srauto informaciją
2. Bendrą tinklo srautą
3. Gautas užklausas ir paketus

FKR-6 Grafinė įspėjimo pranešimo funkcija

1. **Nefunkciniai reikalavimai**

NFR-1 Komponento stebėjimo GUI turi būti naršyklės programa, galinti veikti „Mozilla Firefox“ ir „Google Chrome“ aplinkose.

NFR-2 Šio modulio įgyvendinimas apima:

1. Atakų užklausų klasifikavimą ir treniravimą naudojant PCAP failus
2. Infrastuktūros struktūrizavimą: naudojamos Virtualios mašinos imituoja normalų ir DDoS srautą.

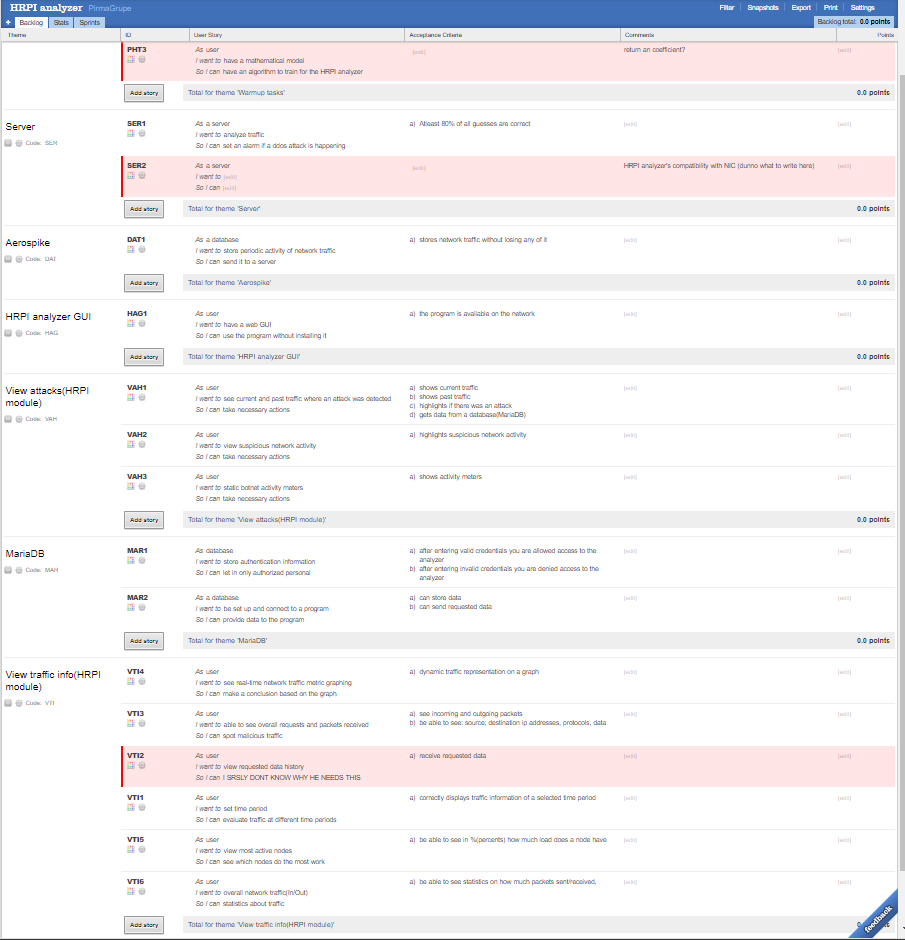
# URL ir prisijungimo duomenys į projekto valdymo įrankį/paskyrą.

[https://easybacklog.com](https://easybacklog.com/)

E-mail: gaming\_fun@mail.com

Password: 7PDmy8E(C76TM`{J

# Backlog veiklos



4 pav. Projekto valdymo įrankio iškarpa

# URL ir prisijungimo duomenys į pasirinktą projekto kodo saugyklą.

<https://github.com/sarand2/ELITNET1>

1. <https://www.hindawi.com/journals/jcse/2013/821315/>, Žiūrėta 2018 03 15 [↑](#footnote-ref-1)