

**Kauno technologijos universitetas**

Informatikos fakultetas

Programų inžinerijos 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

# 

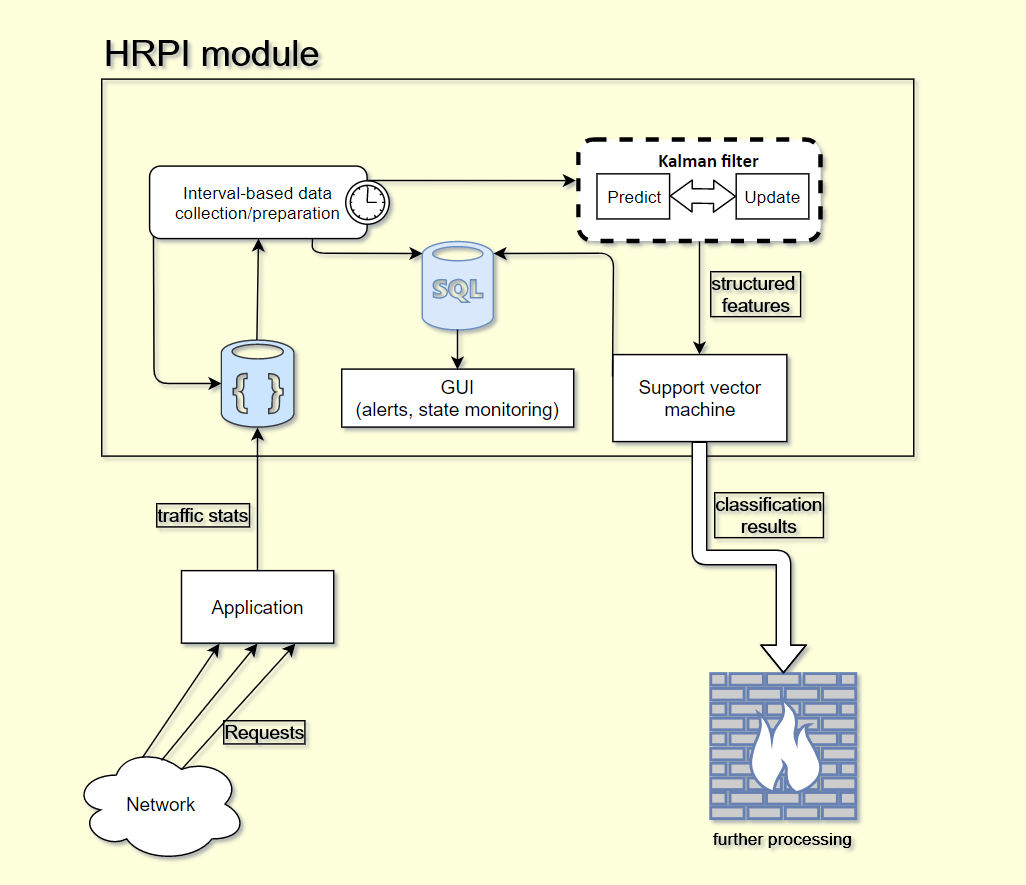
# Įvadas

# Užduotis

Pagal nurodytą matematinį metodą, sukurti HRPI (HTTP *get* Requests Per Ip) analizavimo program, leidžiančią realiu laiku aptikti aplikacijos sluoksnio DDoS atakas. Iš esmės programa turi veikti kaip vienas iš L7 ugniasienės modulių, skirtų HTTP protokolu paremtoms atakoms aptikti.

Šio komponento tikslas – pateikti efektyvią, realiu laiku galinčią veikti sistemos struktūrą bei sąveikaujančias apdorojimo funkcijas, klasifikuojančias programos lygio DDoS atakas. Programa taip pat turi pateikti sistemos administratoriams paprastą naudoti grafinę sąsają tinklo srauto stebėjimui.

Pagrindinės funkcijos:

* 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.
* Būsenos stebėjimas. Analizatorius teikia intuityvias tinklo srauto stebėjimo galimybes, atakos įspėjimo sistemą, ankstesnių būsenų grafikus ir manipuliacijas su istoriniais duomenimis.

# Projekto eiga

## Agile

### Pirmas Sprintas



### Antras Sprintas

### Burn down grafikas

# Retrospektyva

* Individualus darbas prie atskirų sistemos komponentų leido susikoncentruoti į sritį ir pasiekti pakankamai gerus rezultatus kodo įgyvendinimo atžvilgiu, perprasti galimas problemas sąveikoje/komunikacijoje su kitais sistemos komponentais.
* Nestruktūruotas planavimas ir aiškių *deadline* nebuvimas lėmė, kad prie komponentų buvo praleidžiama daugiau laiko, sudaroma daugiau specifinės paskirties kodo, kuris nėra esminis sistemos komponentams.
* Reikėtų daugiau komunikacijos tarp užduočių ir dažnesnio esamo projekto dizaino/veikimo/tobulinimo aptarimo bendrai architektūrai įvertinti.
* Reikėtų mažiau koncentruotis ties naudojamomis technologijomis ir metodais, o bandyti kuo greičiau įgyvendinti specifinį projekto dalies funkcionalumą.

# UML panaudos atvejų diagrama