# SafeGuard模块详细设计

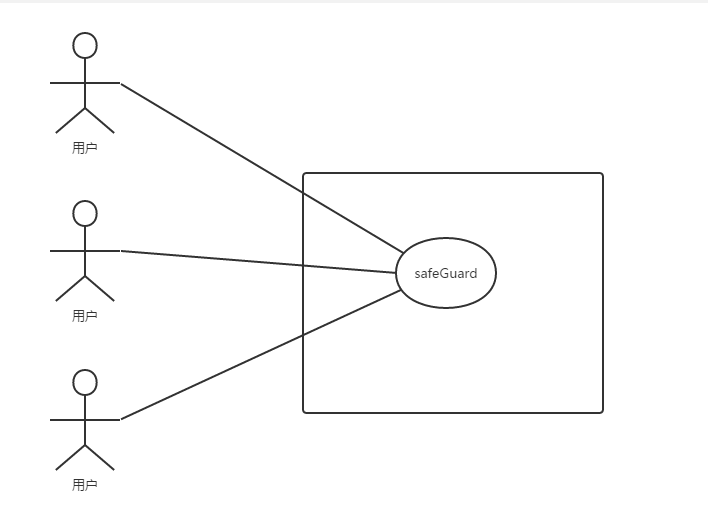
## 概述

模块需求：该模块负责保证服务器安全。用户访问服务器时需要先通过服务器检测模块，屏蔽特定IP以及访问过于频繁的IP（插件扫描攻击）。并且该模块支持可能的入侵检测规则扩展。

涉及需求：

R3 系统安全性 屏蔽99%以上的插件扫描攻击和特定的IP 促进C4

R4 入侵检测可拓展性 增加新的检测规则所需时间低于0.25人月



说明：用户的请求到达SearchProcessor模块前需要先通过SafeGuard模块进行处理

**可能会发生的修改实现**

所屏蔽的特定IP的列表

系统安全检测方法

**分配职责**

1. 该模块将用户访问中可能出现的不安全行为屏蔽，确保服务器的安全和效率

**对外接口：**

接口：Int doSafeCuard(HttpRequest request） ()

功能：当用户的请求到达系统时，首先调用该接口，该接口将返回对该IP访问的检查结果，如果检查通过，则调用模块继续向下调用，否则屏蔽该次访问

**参数说明：**

HttpRequest request：用户请求信息，含有用户的IP、访问时间、mac地址、访问目标等

**返回值说明：**从0至5，分别表示危险评级，屏蔽3级及以上危险评级的访问

**使用方法：**

每当一个用户向服务器请求数据的时候，调用该模块检查用户是否符合访问安全要求，

**前置条件：**

传入的request中包含用户IP、mac地址、访问时间、访问目标

**后置条件**

1、返回对该次访问的安全评级

2、对储存的数据进行修改，更改某些IP地址的访问记录以及安全评价

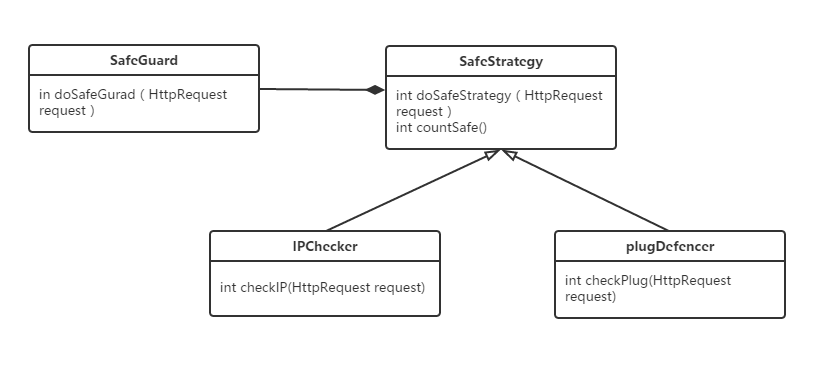
**设计方案分析**

用户的请求到达的时候，SafeGurad模块调用SafeStrategy模块进行访问分析，SafeStrategy模块则依此调用继承自SafeStrategy模块的安全策略模块，目前拥有的是IPCheck模块和PlugDefence模块

## 2类图

**静态结构**

**详细设计类图和类图说明：**



设计说明：该模块主要由两个部分组成：SafeGuard 和SafeStrategy

HttpRequest通过SafeGuard类传入SafeStrategy类，再通过SafeStrategy类调用其子类，最后通过子类返回值计算出该次request的安全评级并返回

## 3类描述

**类方法（重要方法要给出前置与后置条件）与重要数据结构描述**

|  |  |
| --- | --- |
| 类 | 说明 |
| SafeGuard | 传入HttpRequest对象，向下传递并获取返回结果 |
| SafeStrategy | 安全策略类，为所有策略的父类，调用所有策略，计算结果并返回 |
| IPChecker | 策略类的子类，检查IP是否在屏蔽列表内 |
| PlugDefencer | 策略类的子类，检查该次访问是否是插件扫描攻击 |

|  |  |
| --- | --- |
| SafeGuard | |
| DoSafeGuard | 获取HttpRequest向下传递并获取返回值 |

|  |  |
| --- | --- |
| SafeStrategy | |
| doSafeStrategy | 调用所有的检查策略，并返回该次访问的危险值 |
| CountSafe | 计算该访问的危险并返回 |

|  |  |
| --- | --- |
| IPChecker | |
| checkIP | 检查IP是否合法 |

|  |  |
| --- | --- |
| PlugDefencer | |
| checkPlug | 检查该次访问是否是插件扫描攻击 |

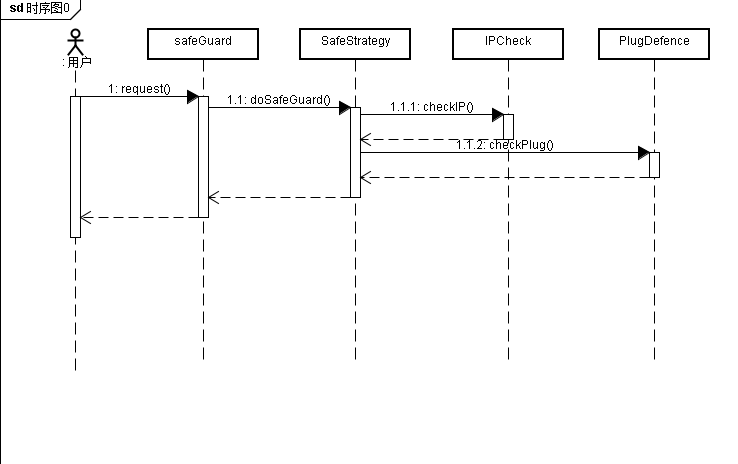
**重要的数据结构描述**

用户请求

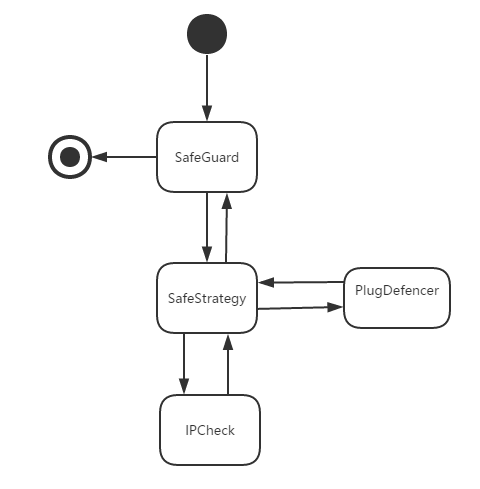
HttpRequest：其中有用户IP、mac地址、访问时间、访问目标

## 4重要协作

**顺序图**



**状态图**



## 5使用的设计模式

**策略模式：**模块含有一个策略的调用者SafeStrategy和若干个继承自SafeStrategy的安全策略类，SafeGuard调用SafeStrategy类，由safeStrategy类调用其记录的所有策略类。当安全检查策略发生修改或删除时，只需修改对应的策略类，当增加安全策略时，只需要增加安全策略类，并在SafeStrategy类中增加该类的调用

**场景：**检查用户的访问安全

**目的：**屏蔽不安全的请求