**Computer Systems Technology**

British Columbia Institute of Technology

COMP 8006 - Assignment3- Design

Albert Huang &

Aiyan Ma

Feb 28, 2018

# Table of Contents

[Table of Contents 1](#_Toc28550)

[Design 3](#_Toc20239)

[1.1 Introduction 3](#_Toc18023)

[1 Configuration 3](#_Toc4856)

[2 Monitoring: 3](#_Toc30763)

[3 Action 4](#_Toc32721)

[4 Unblock 4](#_Toc15182)

[1.2 Flowchart 4](#_Toc26875)

[1.2.1 Main Flow 4](#_Toc31035)

[1.2.2 Config Flow 6](#_Toc32370)

[1.2.3 monitor variables config 8](#_Toc18061)

[1.2.4 Others 9](#_Toc28867)

# Design

## 1.1 Introduction

There are four modules designed as:

1. Configuration ( Config)
2. Monitoring
3. Action
4. Unblock

### 1 Configuration

In terms of the Config, it provides a GUI for user to input and config the required parameters:

1) Setup the monitor variables as log file location, Maximum password attempts allowed, blocking interval, service by port and keywords etc.

2) IP address Handling;

It provides 2 ways for Ip address handling: one is by location( fields number of the record in the log file) and the 2nd way is by regular expression. It also very nice to provide a system default pattern can be applied for almost all the cases. Of course, user defined patterns also supported. Due to the error pron design, a test ( verify) function is provided for end use to test the pattern before really applied in it.

### 2 Monitoring:

Monitoring is done dynamically to get the incremental part of the logs and make the analysis for the sensitive words are in or not.

If the critira triggered, the client IP, times attempted is recorded to compare with the threshold. If the threshold reached, the action will be taken.

This module is taking advantage of Array to store the records, using the crontab to invoke the Unblock action when time is up.

### 3 Action

Action here is designed to do the real action for malicious activities. In this case, it means to block the connection when asked by the monitor module.

It calls the *iptables* to setup the rule to indeed take the action.

### 4 Unblock

Unlbock is triggered automatically by crontab when the time limit is reached. When it’s time to unblock, the crontab job is cleared and the rules on the firewall is removed to allow the access again.

## 1.2 Flowchart

### 1.2.1 Main Flow

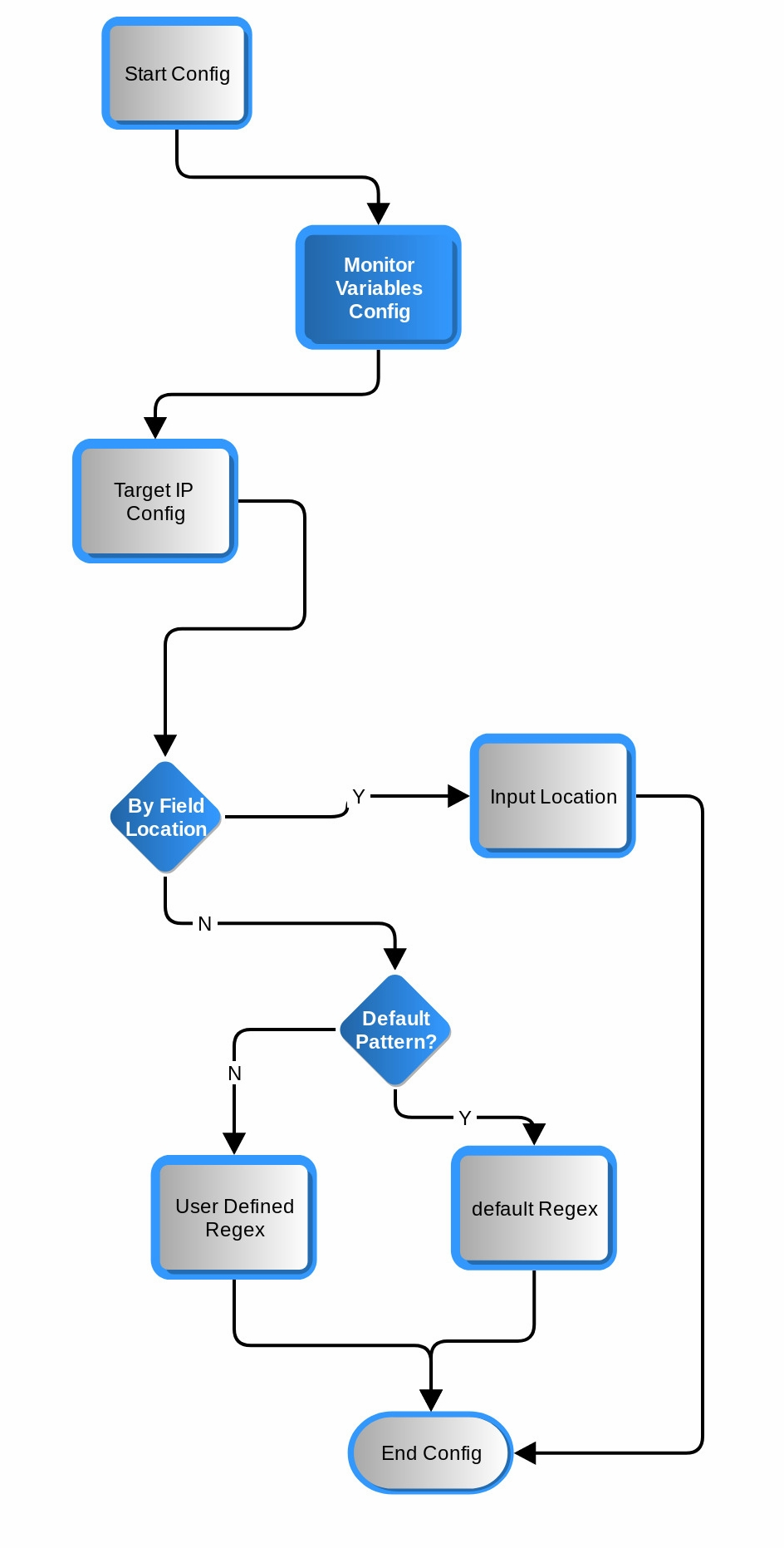
Main Flow can be seen as below, it starts from config, the monitor module is at the heart of it:

## 

### 1.2.2 Config Flow

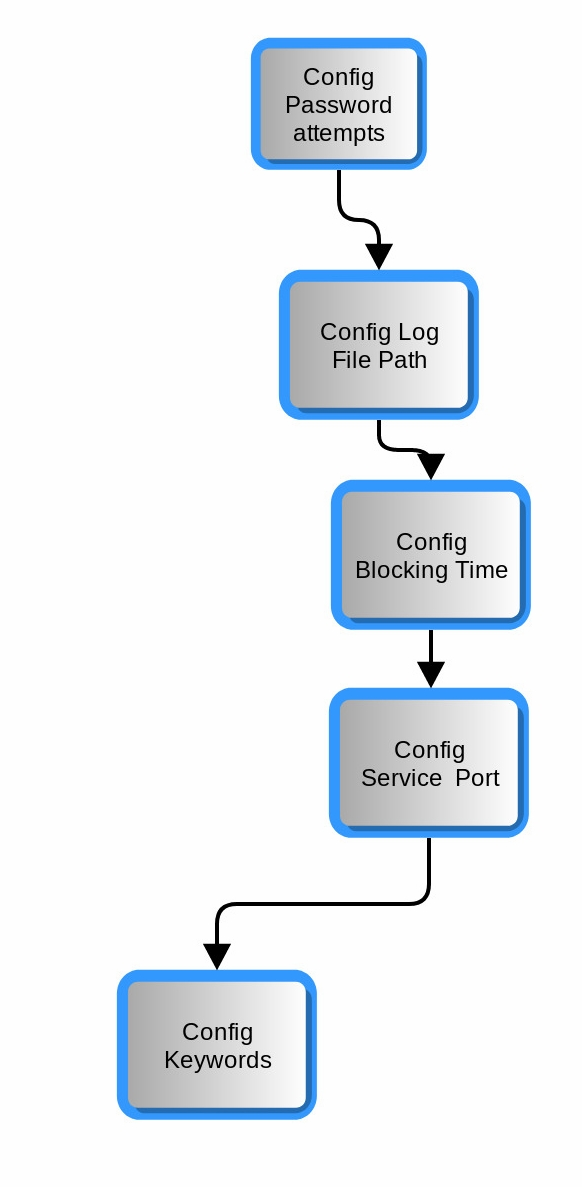
In terms of the config, it has intensive user action required, if compared with other modules which are more in slient mode.

To star the config:



### 1.2.3 monitor variables config

As for the monitor variables config, it shows the flow chart as below:



### 1.2.4 Others

Other functions as actions and unblock are pretty straight forward thus no more flow chart required. There is also a function for showing the black list which is simply display the array content thus no more explanation in the design doc. It will be shown in the test documentation.