Documentation for the HSP project “LogAnalyzer”

By Philipp Rieger, Andreas Kalo Fogados, Michael Dorr

Date: WS 15/16

Examiner: Prof. Dr. Skornia

# 1 Environment Setup

## 1.1 Log Production via RADIUS Server and Syslog

## 1.2 Database Setup

## 1.3 Project Structure

The hierarchy of the project is as following:

* src: this folder contains all source and header files
* files: the directory lists different files such as log files or test files that were made use of during the development
* bin: folder with the final binary file
* Makefile: file that builds the source files and stores the binary in the bin folder when the “make” command is issued

The development process of the project was performed on a Linux virtual machine, more specifically Ubuntu 14.04, that was running the mongo db service. Furthermore, Git was used as a version control system to simplify the distributed work.

# 2 Implementation Details

The application reads content from log files and stores them into the database. The analyzer starts by reading those log contents from the mongo database and applying a regular expression in order to build login record objects.

As a further step, the application filters information from these records to build user objects that are, in turn, stored in the repository. Thereafter, the analyzer goes ahead with determining the handy mac address for each user based on the frequency of its appearance in the user’s login records.

Eventually, the standard deviation of all considered entries is calculated and further used to check if any anomalies occurred.