Log Data Visualization

Gabrielle Talavera
Advisor: Eduardo Jacob
Department of Computer Science & Engineering
University of Nevada, Reno

Introduction

For end-to-end strong authentication and authorization solutions which generate a great amount of system information via system logs, it is important to treat, store, and visualize the interactions between the elements, to analyze and evaluate how the system is working and what are the trends. To address this issue, the Kibana data visualization plugin for Elasticsearch will be employed.

Hidra Security Protocol

Hidra is a security protocol that guarantees both the authentication and authorization of a remote subject wanting to access a service in a constrained device sensor (CDS). As shown in Figure 1, there are four phases involved. This project focuses on phase 4 (Access Notification) which is where the CDS sends to the central architecture the details about the access attempts, enabling centralized logging and accounting.

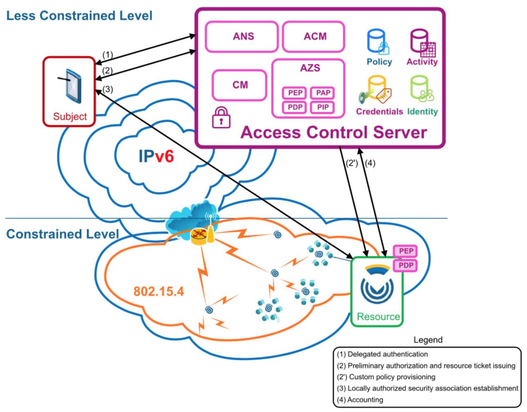

Figure 1: Hidra Security Protocol Phases

Methodology

The goal was to visualize the log data from phase 4 of the Hidra Security Protocol. ,Elasticsearch, a search engine, and Kibana, a data visualization plugin, were found to be the best options to reach this goal. After downloading all the needed software, a predefined dataset of systems logs was created using Microsoft Excel. The data was then imported to Kibana, and from there the visuals were created and placed on the dashboard. The graphics created were the total requests, the total amount of permitted accesses and denied access, requests per subject, requests per applied policies, requests per applied rules, and the requests per resource.

Figure 2: Importing Data in Kibana

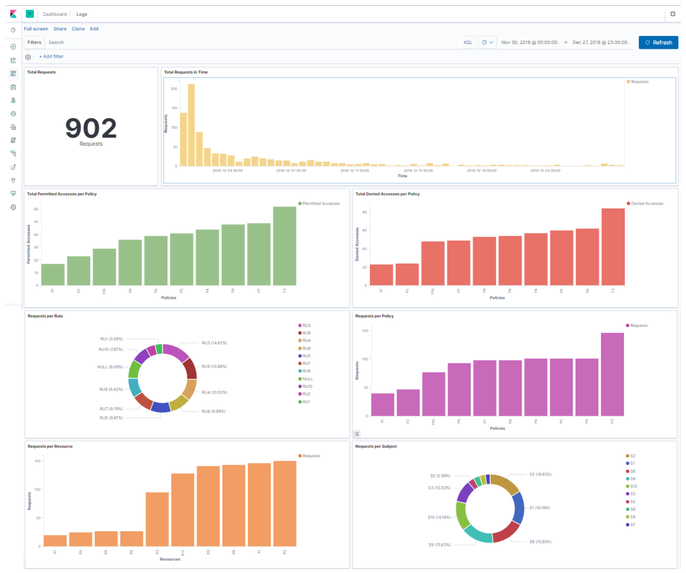

Figure 3: Completed Kibana Dashboard

Conclusion

This project visualized log data from a predefined dataset onto a dashboard. This is important for the Hidra Security protocol because it allows for analyzation and evaluation of how the system works and its trends. Thanks to this powerful security mechanism for CDS, more IoT applications will be possible to be implemented and used by the society in a secure way.

Future Work

An extension of this project is to incorporate log data in real time rather than coming from a predefined dataset. To accomplish this the ELK stack which consists of Elasticsearch, Logstash, and Kibana would be used. Logstash is a data processing pipeline which would ingest logs and send data to Elasticsearch in a continuous, streaming fashion. This would allow for the data visualizations to constantly be updated as logs are being created which is beneficial in monitoring the data in real time.

Acknowledgements

This work was supported by UNR's Office of Undergraduate Research. I would like to thank Ane Sanz Rekalde, Jasone Astorga, Maider Huarte, and Eduardo Jacob for providing me with their guidance and support throughout this project.